INTERNAL AUDIT IN THE DIGITAL AGE

CONCEPTS, CASES, AND APPLICATIONS

Book Series

Contemporary Studies in Business and Management

Edited by Tuğçe Uzun Kocamış, Ali Kuzu & Serap Özdemir Güzel

Volume I

Internal Audit in the Digital Age: Concepts, Cases, and Applications

Tuğçe Uzun Kocamış

Internal Audit in the Digital Age:

Concepts, Cases, and Applications

maurer.press
Frankfurt am Main

Bibliografische Information Der Deutschen Nationalbibliothek

Die deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie: detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar

maurer.press

is an imprint of
Verlag Hans-Jürgen Maurer
Im Trierischen Hof 14
60311 Frankfurt/Germany
www.maurer.press
GPSR-Kontakt: info@maurer.press
ISBN 978-3-949550-36-2
e-ISBN 978-3-949550-37-9

Table of Contents

PART II

DIGITAL RISKS, CONTROLS AND TECHNOLOGIES

PART III

INTERNAL AUDIT CASES AND APPLICATIONS

Preface

The contemporary business environment is characterized by increasing complexity, driven by digital transformation, intensified global competition, expanding risk exposure, and growing regulatory expectations. These developments have significantly reshaped the role and relevance of internal audit and internal control functions. Internal audit is no longer understood merely as a traditional control activity concerned with detecting errors, irregularities, or compliance deficiencies. Rather, it has evolved into a strategic assurance and advisory function that supports corporate governance, evaluates risk management practices, strengthens ethical culture, and contributes to organizational value creation.

This book examines the transformation of internal audit in the digital age from both theoretical and practical perspectives. It addresses the fundamental concepts of internal audit, internal control systems, risk-based auditing, corporate governance, digital audit tools, cybersecurity, artificial intelligence-supported audit practices, and case-based applications. By adopting a holistic approach, the book aims to demonstrate how internal audit has become an essential component of modern governance and risk management structures.

The primary objective of this book is not only to provide conceptual knowledge, but also to offer a practical framework for understanding how internal audit can be applied in contemporary organizations. In this respect, it is intended to serve as a useful resource for students, academics, internal auditors, external auditors, risk managers, control specialists, and professionals working in the field of corporate governance. As digitalization continues to transform business processes, the competency profile of internal auditors is also changing. Internal auditors are now expected to go beyond traditional accounting and auditing knowledge and develop capabilities in data analytics, information technologies, cybersecurity, ethical reasoning, and professional communication.

Accordingly, the future of internal auditing depends on a risk-oriented and value-creating audit approach that integrates human judgment with technological tools. It is hoped that this book will contribute to both the academic literature and practical understanding of internal auditing in the digital age.

Introduction

Contemporary organizations operate in an environment shaped by intensified global competition, increasing financial and operational risks, stronger regulatory expectations, and the rapid diffusion of digital technologies. These developments have substantially changed the role of internal audit and internal control. Internal audit is no longer limited to the retrospective examination of transactions, the detection of errors and irregularities, or the verification of compliance with rules and procedures. It has increasingly become a strategic assurance and advisory function that contributes to corporate governance, risk management, ethical culture, cybersecurity, digital transformation, and organizational value creation.

The historical development of internal auditing reflects this transformation. Initially, internal audit emerged as a mechanism for protecting assets, reducing record-keeping errors, and preventing fraud. Over time, however, its scope expanded beyond financial verification to include management control, operational effectiveness, risk management, and the evaluation of governance processes (Ramamoorti, 2003). This evolution is closely associated with the separation of ownership and management, the growth of transaction volume, the increasing complexity of business operations, and the need for reliable information in decision-making. As organizations became larger and more complex, management and stakeholders required an independent assurance mechanism capable of evaluating both financial and operational activities. In this respect, internal audit gradually moved from an activity performed "for management" to a broader function that also examines management systems, controls, and governance structures (Ramamoorti, 2003).

The role of internal audit in corporate governance became particularly visible after major corporate scandals such as Enron and WorldCom. These failures demonstrated that external audit alone is not sufficient to ensure accountability and transparency. Effective governance requires the coordinated operation of internal control systems, internal audit, audit committees, executive management, and boards of directors. Within this structure, internal audit serves as an important

governance mechanism by providing independent and objective assurance to the board, audit committee, senior management, and other stakeholders. While corporate governance aims to ensure that an organization is managed transparently, responsibly, fairly, and accountably, internal audit evaluates whether these principles are effectively embedded in organizational practices (Alwyah, 2025; Laflafli & Saidi, 2025).

The literature also shows that internal audit is not a one-dimensional activity. Internal auditors provide assurance on governance, risk management, and internal control processes, while also offering advisory support for process improvement, efficient resource use, and organizational performance. However, this multi-role structure can also create ambiguity regarding the boundaries and core identity of internal audit. Roussy and Perron's structured literature review identifies three major themes in internal audit research: the multiple roles of internal audit, internal audit quality, and internal audit practice. Their study also emphasizes that internal audit is sometimes perceived as a governance actor expected to address nearly every organizational issue, although its actual role, quality criteria, and practical boundaries still require further clarification (Roussy & Perron, 2018).

For this reason, the value of internal audit should not be measured merely by the production of audit reports. Rather, its value lies in the extent to which it supports the achievement of organizational objectives. Internal audit creates value when it strengthens governance, improves the effectiveness of internal controls, helps identify risks at an earlier stage, reduces fraud risk, and provides reliable information for decision-making. Recent studies indicate that stakeholders associate the contribution of internal audit to governance, internal control, and risk management with organizational value creation. However, this value should be assessed not only from the perspective of internal auditors themselves, but also in light of the expectations of audit committees, senior management, boards of directors, and other stakeholders (Amo et al., 2026).

Internal control constitutes the fundamental structure within which internal audit operates. It refers to the set of policies, procedures, and

practices designed to safeguard assets, ensure the reliability of financial and operational information, support effective and efficient operations, and secure compliance with laws and regulations. Historically, internal control was primarily associated with the accuracy of accounting records and the prevention of errors. In contemporary organizations, however, it has evolved into a broader managerial system linked to risk management, information production, decision-making, and organizational sustainability. The COSO framework conceptualizes internal control as an integrated structure composed of five interrelated components: control environment, risk assessment, control activities, information and communication, and monitoring activities (Ferdia & Kammoun, 2024).

The relationship between internal audit and internal control is reciprocal and complementary. Internal control operates as a managerial mechanism that reduces risks in day-to-day activities and supports the orderly functioning of business processes. Internal audit, by contrast, independently evaluates the adequacy, design, and operating effectiveness of that system. Weak internal controls may result not only in operational errors, but also in financial reporting problems, asset losses, regulatory breaches, and fraud risks. A strong internal audit function contributes to organizational resilience by identifying control deficiencies, communicating them to management, and supporting corrective action (Shah et al., 2023).

Fraud risk management is one of the most critical areas in which internal audit contributes to organizational governance. Fraud is not merely a financial irregularity; it is also a governance failure that can damage reputation, stakeholder trust, ethical culture, and the efficient use of organizational resources. Studies conducted in both public and private sector contexts show that internal audit plays an important role in fraud prevention, detection, and reporting. In particular, the relationship between internal audit quality, ethical behavior, and organizational culture suggests that fraud management should not be treated solely as a technical control issue. It must also be considered in relation to ethical norms, social behavior, and organizational values (Mintah et al., 2025; Kabuye et al., 2026).

Ethical culture is therefore a central determinant of internal audit effectiveness. Internal audit should not be limited to testing whether controls exist; it should also contribute to the development of integrity, accountability, fairness, responsibility, and ethical conduct within the organization. The finding that ethical behavior strengthens the relationship between internal audit quality and fraud management indicates that internal audit is not only a structural or technical function, but also a behavioral and cultural governance mechanism. Accordingly, an effective internal audit system should be evaluated together with independence, competence, professional standards, and an organizational climate that supports ethical conduct (Kabuye et al., 2026).

Independence and objectivity are among the core principles that sustain the credibility of internal audit. Nevertheless, because internal auditors operate within the organization, their independence is not absolute or free from tension. Internal auditors are expected to provide advisory support to management while also independently evaluating management's activities, decisions, and control systems. This dual role creates a persistent challenge. Recent studies indicate that internal auditors use various tactics to protect, model, and extend their independence in order to maintain their position as a third-line assurance provider within the organization (Eklöv Alander & Holmgren Caicedo, 2026).

Digital transformation has further expanded the scope, methods, and expectations of internal audit. Financial transactions, procurement, inventory management, human resources, customer relations, and reporting processes are increasingly carried out through digital platforms and integrated information systems. As a result, the nature of audit evidence has changed. Physical documents, manual approvals, and periodic reports are now complemented by system logs, ERP records, electronic approval trails, automated control reports, database outputs, and real-time transaction traces. Digital transformation therefore makes audit processes more data-intensive, analytical, and continuous (Ma & Zhang, 2026).

The impact of digital transformation on internal audit quality can be understood as the result of a mutually reinforcing relationship

between human capability and technological infrastructure. Digitalization increases the need for internal auditors to acquire competencies in areas such as data literacy, information systems, analytical thinking, artificial intelligence, and cybersecurity. These competencies allow auditors to interpret digital evidence more effectively and to evaluate technology-based risks with greater professional judgment. In parallel, investments in digital infrastructure expand the operational capacity of internal audit by enabling the use of data analytics platforms, automation tools, and real-time monitoring systems. When auditor expertise and technological resources are aligned, internal audit can achieve higher levels of audit quality, efficiency, and responsiveness (Ma & Zhang, 2026).

Artificial intelligence, machine learning, and data analytics are among the most influential technologies shaping the future of internal audit. Traditional audit approaches largely rely on sample-based testing, whereas advanced analytics and machine learning techniques enable auditors to examine full populations of transactions. These technologies support anomaly detection, continuous auditing, process mining, predictive risk assessment, and automated transaction testing. AI-assisted auditing can help identify high-risk transactions earlier, allocate audit resources more effectively, and provide a stronger analytical basis for audit findings (Shivram, 2024).

However, the use of technology also introduces new risks. Explainability, data quality, algorithmic bias, professional skepticism, ethical oversight, and the preservation of human judgment are critical concerns in AI-supported audit environments. Audit technologies do not remove the auditor's responsibility for professional judgment. On the contrary, they increase the need for auditors to critically evaluate technological outputs, interpret model results, and place findings within the broader organizational context. In this sense, the digital auditor is not a passive user of technology, but a professional judgment actor who governs technology-supported assurance processes (Shivram, 2024).

Cybersecurity has also become one of the most strategic areas of internal audit in the digital age. As organizations become increasingly

dependent on digital infrastructures, they are exposed to risks such as data breaches, ransomware, phishing, unauthorized access, system disruption, and information leakage. Internal audit must therefore evaluate not only financial controls, but also IT governance, cybersecurity policies, data privacy compliance, access controls, and incident response processes. The quality of cybersecurity auditing is closely associated with the IT expertise of the chief audit executive, direct communication with the audit committee, strong IT governance, and the regular review of cybersecurity policies by internal audit (Alzeban et al., 2026).

Blockchain technology also has the potential to transform audit practices. By enabling transactions to be recorded in an immutable, transparent, and traceable manner, blockchain can enhance the reliability of audit trails. It may contribute to transaction verification, record integrity, real-time monitoring, and the reduction of intermediary dependence. However, blockchain-based auditing also creates challenges related to regulatory compliance, data privacy, interoperability, and technical complexity. Therefore, the integration of blockchain into audit processes should be treated not merely as a technological innovation, but also as a governance and risk management issue (Syahputra, 2022).

The effectiveness of internal audit also depends on organizational culture, human interaction, and behavioral factors. The audit process often creates an asymmetric relationship between auditors and audited units. Auditees may perceive audit as a threat, criticism, or punitive mechanism, which can limit information sharing, cooperation, and acceptance of findings. For this reason, internal audit is not only a procedural and documentation-based activity; it also requires communication, trust, empathy, persuasion, ethical awareness, and emotional intelligence. Audit effectiveness depends not only on technical knowledge, but also on the quality of the relationship between auditors and auditees (Wronka, 2019).

Cultural context is another factor that influences internal audit practice. In multinational organizations, national differences in power distance, uncertainty avoidance, future orientation, communication

style, and perceptions of authority may affect how internal audit standards are implemented. In high power-distance environments, internal auditors may find it more difficult to challenge senior management or maintain a critical stance. In cultures that support open and assertive communication, auditors may be better able to raise risks and defend professional judgments. Thus, while international internal auditing standards provide a common global framework, their implementation cannot be separated from cultural and institutional contexts (Hallak & Feghali, 2026).

This book examines the transformation of internal audit in the digital age through a multidimensional approach. Its central argument is that internal audit can no longer be understood solely as compliance testing, error detection, or financial control evaluation. It should instead be viewed as an integrated assurance and advisory function linked to corporate governance, internal control, risk management, ethical culture, fraud prevention, cybersecurity, digital transformation, artificial intelligence, blockchain, and human behavior. The book first explains the historical and theoretical foundations of internal audit, then examines its relationship with internal control, corporate governance, risk management, and digital technologies, and finally applies these concepts through case analyses.

The purpose of the book is not only to present conceptual knowledge, but also to provide a practical framework for understanding how internal audit can be applied in digitally transformed organizations. It is intended as a resource for students, academics, internal auditors, external auditors, risk managers, control specialists, information systems auditors, and professionals working in the field of corporate governance. By addressing topics ranging from the historical evolution of internal audit to AI-assisted auditing, from internal control systems to cybersecurity audits, and from fraud cases to ethical issues, the book aims to offer both academic and practice-oriented value.

In conclusion, internal audit in the digital age is moving away from a retrospective control function focused on detecting past errors. It is becoming a forward-looking strategic function that provides assurance, anticipates risks, uses technology, supports ethical culture,

strengthens governance, and contributes to organizational value. This transformation requires internal auditors to possess not only accounting and auditing knowledge, but also competencies in data analytics, information technology, cybersecurity, artificial intelligence, communication, ethical reasoning, and cultural awareness. The future of internal audit depends on a risk-based, continuous, data-driven, and value-creating assurance approach in which human judgment and digital

PART I

FOUNDATIONS OF INTERNAL AUDIT IN THE DIGITAL AGE

Chapter 1 – Fundamentals of Internal Audit

Introduction

Internal audit in modern organizations has evolved from a traditional control activity focused mainly on financial records into a strategic assurance and advisory function. As businesses grow, operations become more complex, and technological systems become increasingly central to business processes, the scope of internal audit has expanded significantly.

Today, internal audit is closely linked to risk management, internal control, corporate governance, ethical culture, operational efficiency, and digital assurance. Internal auditors are no longer expected only to identify errors, irregularities, or compliance deficiencies. They are also expected to evaluate risks, assess the effectiveness of controls, provide recommendations for process improvement, and support value creation within the organization.

This chapter discusses the definition and objectives of internal audit, its relationship with corporate governance, internal control systems, the risk-based audit approach, and the changing role of internal auditors in modern organizations. The chapter aims to show that internal audit is not merely an activity that detects errors and fraud, but an integrated assurance function that adds value to the organization, anticipates risks, and supports sound governance.

1.1. Definition and Objectives of Internal Audit

Internal audit historically arose from the need to prevent errors, fraud, asset loss, and record inaccuracies in businesses; over time, it transformed from a narrow activity that only checked financial transactions into a strategic assurance function that evaluates the risk

management, internal control, and corporate governance processes of the company (Ramamoorti, 2003).

The modern understanding of internal audit is not limited to examining only the past transactions of the company; it also aims to identify potential future risks, improve control systems, and provide recommendations that add value to management. According to the IIA's contemporary definition of internal audit, internal audit is an independent and objective assurance and advisory activity carried out to add value to and improve the operations of an organization. This activity aims to evaluate and improve the effectiveness of risk management, control, and governance processes with a systematic and disciplined approach (Laflafli & Saidi, 2025).

This definition shows that internal audit is not just a mechanism that looks for errors, but a professional management function that contributes to the achievement of the company's objectives. The fundamental objectives of internal audit include evaluating the adequacy of the internal control system, improving the effectiveness and efficiency of operations, ensuring the reliability of financial and operational information, monitoring compliance with legislation and internal policies, contributing to the protection of assets, and providing management with reasonable assurance about risks (Shah et al., 2023; Ramamoorti, 2003).

In this respect, internal audit is an assurance mechanism that supports both the financial and operational sustainability of the company. In the digital age, the objectives of internal audit have further expanded. Internal auditors no longer only review accounting records or manual controls; they also evaluate information systems, data security, digital transaction trails, automated controls, cyber risks, and technology-based processes. The inclusion of technologies such as blockchain, data analytics, and artificial intelligence in audit processes is transforming the scope of internal audit into a more analytical, continuous, and real-time structure (Syahputra, 2022).

1.2 Internal Audit and Corporate Governance

Corporate governance refers to the management of businesses in accordance with the principles of transparency, accountability, responsibility, fairness, and independence. An effective corporate governance system aims to reduce conflicts of interest between business management and stakeholders, make decision-making processes reliable, and protect business value (Luckyanayu et al., 2025).

Internal audit is considered one of the fundamental elements of the corporate governance system. In the literature, internal audit is considered one of the main oversight mechanisms of corporate governance, along with management, the audit committee, and external audit (Alwyah, 2025). The internal audit function provides reliable information to the board of directors, the audit committee, and senior management by independently evaluating the activities carried out within the company.

The relationship between corporate governance and internal audit can be explained particularly in the context of information asymmetry and the agency problem. According to agency theory, conflicts of interest may arise between business owners and managers because managers may not always act in the interests of shareholders. In this context, internal audit gains importance as a mechanism that monitors, controls, and reassures stakeholders about the activities of managers (Alwyah, 2025; Laflafli & Saidi, 2025).

Internal audit contributes to the strengthening of corporate governance through its assurance and advisory functions in relation to internal control, risk management, and ethical compliance. By evaluating the design and operating effectiveness of internal control systems, internal audit enhances accountability within the organization. Furthermore, its assessment of risk management practices provides management with more reliable information for informed decision-making. Internal audit also functions as an early warning mechanism by identifying potential indicators of unethical behavior, irregularities, and fraud before they escalate into significant governance failures (Luckyanayu et al., 2025; Mintah et al., 2025).

There is a positive relationship between the quality of corporate governance and the quality of internal audit. A strong corporate governance structure increases the independence and effectiveness of internal audit; and quality internal audit contributes to the increase in business value (Zhao & Xu, 2025). Therefore, in modern businesses, internal audit is not only a technical unit that provides control, but also a strategic part of the corporate governance system.

1.3. Internal Control Systems

An internal control system is the entirety of policies, procedures, methods, and practices created to support the achievement of a company's objectives. Internal control is a fundamental management tool in terms of protecting assets, ensuring the reliability of financial information, conducting operations effectively and efficiently, and ensuring compliance with legislation (Ferdia & Kammoun, 2024).

The concept of internal control has undergone a significant transformation over time. Initially focusing more on preventing errors and fraud, ensuring the accuracy of accounting records, and protecting assets, the understanding of internal control has evolved into a more comprehensive structure with the growth of businesses, the increasing complexity of operations, and the increased use of technology. Today, internal control is not only related to the accounting system; it is considered an integrated system encompassing all the activities, risks, information flow, and monitoring mechanisms of the company (Ferdia & Kammoun, 2024).

According to the COSO approach, an effective internal control system consists of five basic components: control environment, risk assessment, control activities, information and communication, and monitoring activities. These components form the control culture of the company and provide reasonable assurance to management (Ferdia & Kammoun, 2024). Internal audit is the fundamental function that evaluates the effectiveness of this system and contributes to its improvement.

Internal control systems have not only a protective but also a preventive and developmental function for businesses. An effective internal control system reduces financial losses, operational errors, regulatory violations, and fraud risks. It also facilitates management's decision-making based on reliable information (Shah et al., 2023).

Digitalization has significantly changed internal control systems. Manual controls are increasingly being replaced by automated controls, system-based approval mechanisms, data analytics-supported monitoring tools, and real-time alert systems. While this increases the effectiveness of internal control systems, it also brings new risk areas such as cybersecurity, access rights, data integrity, and system dependency to the forefront (Syahputra, 2022).

1.4. Risk-Based Auditing

Risk-based auditing is a contemporary auditing approach that focuses on directing internal audit resources to the most important risk areas of the company. While traditional auditing focuses more on examining the accuracy of past transactions, risk-based auditing attempts to identify current and potential risks that may prevent the company from achieving its objectives (Ramamoorti, 2003).

In the risk-oriented approach, the audit plan is prepared according to the risk profile of the company. Therefore, internal auditors determine which processes carry higher risk, which controls are critical, and which areas should be audited as a priority. Thus, the audit activity ceases to be merely a routine control exercise; it transforms into an assurance mechanism aligned with the strategic objectives of the company.

Modern businesses face operational, strategic, technological, compliance, and reputational risks in addition to financial risks. In particular, digital transformation has broadened the risk map; cyberattacks, data breaches, system outages, automated transaction errors, and algorithmic decision-making risks have become new areas of examination for internal auditing (Syahputra, 2022). Risk-based auditing is also an

important tool in managing fraud risks. Internal auditors assess risks such as weak control points that could lead to fraud, unusual transactions, and management circumvention of controls. Regular internal audit activities are considered critical in combating fraud, in terms of preventing, detecting, and reporting fraud risks (Mintah et al., 2025).

The effectiveness of risk-based auditing is closely related to internal auditors' data analytics, process knowledge, and risk assessment competencies. In the digital age, internal auditors can analyze large datasets to detect anomalies earlier and respond to risks in real time through continuous auditing practices. Therefore, risk-based auditing is one of the fundamental building blocks of the digital internal auditing approach.

1.4. The Role of Internal Auditors in Modern Organizations

In modern organizations, the role of internal auditors has gone far beyond the traditional understanding of control. While in the past internal auditors were primarily seen as individuals who examined financial records, cash transactions, accounting documents, and compliance controls; today, they also play an active role in risk management, corporate governance, internal control, process improvement, technology auditing, and strategic consulting (Ramamoorti, 2003).

Internal auditors are professionals who provide independent assurance within the company. This assurance is not only related to the accuracy of financial statements; it also concerns the effectiveness of business processes, the adequacy of controls, the maturity of risk management, and whether the governance structure is functioning properly (Laflafli & Saidi, 2025).

Another important role of modern internal auditors is their consulting function. Internal auditors offer suggestions to management on process improvement, efficient use of resources, cost control, performance measurement, and risk reduction. In this respect, internal auditing has become a function that not only finds errors but also

increases the value creation capacity of the company (Luckyanayu et al., 2025).

The competency profile of internal auditors has also changed in the digital age. Today's internal auditors need more than just accounting and finance knowledge. They also need to be knowledgeable about data analytics, ERP systems, cybersecurity, blockchain, artificial intelligence, automated control systems, and digital reporting tools (Syahputra, 2022).

Internal auditors also play a significant role in strengthening ethical culture and reducing fraud risks. Effective internal audit activities increase employee compliance with rules, make control weaknesses visible, and support a culture of accountability within the company (Shah et al., 2023; Alwyah, 2025).

In conclusion, in modern organizations, the internal auditor is a strategic professional who not only controls but also analyzes, anticipates risks, provides assurance to management, uses technology, and contributes to corporate value. With digital transformation, this role is expanding even further, and the internal audit function is becoming central to the sustainability of businesses.

Chapter Summary

This chapter discusses the fundamental concepts, objectives, and role of internal audit in modern businesses. It emphasizes that internal audit is not merely a traditional control activity that detects errors, fraud, and record inaccuracies; it is an independent and objective assurance function that supports risk management, internal control, and corporate governance processes.

The chapter also explains the relationship between internal audit and corporate governance, internal control systems, and a risk-based auditing approach. It is stated that an effective internal audit function makes significant contributions to businesses in terms of transparency, accountability, regulatory compliance, asset protection, and process improvement.

Finally, the impact of digitalization on internal audit is evaluated; it is stated that areas such as ERP systems, data analytics, automated controls, artificial intelligence, and cybersecurity have expanded the duties and competencies of internal auditors. In this context, internal audit stands out as a strategic management tool in modern organizations that adds value to the company, anticipates risks, and supports

Chapter 2 – Digital Transformation and the Audit Environment

Introduction

Digital transformation has significantly changed the way businesses operate, their control structures, and their audit processes. Manual and paper-based processes are being replaced by ERP systems, cloud computing, big data analytics, artificial intelligence, blockchain, and automated controls. While these developments have made audit activities faster, more comprehensive, and data-driven, they have also created new audit areas such as cybersecurity, data integrity, access rights, and algorithmic risks.

This chapter addresses digitized business processes, the impact of Industry 4.0 on auditing, cloud systems, remote auditing applications, ERP systems, and digital risks. The aim of the chapter is to explain how the audit environment has changed in the digital age and how internal auditors should adapt to this new environment.

2.1. Digitalization of Business Processes

Digitalization transforms businesses' business processes from manual, paper-based, and fragmented structures to data-driven, integrated, and technology-supported structures. This transformation is not only about transferring existing processes to electronic environments; it also includes the redesign of production, sales, accounting, financial reporting, supply chain, internal control, and audit processes. Businesses use digital technologies to generate information faster, increase communication between processes, and make decision-making processes more analytical (Leng & Zhang, 2024).

Among the most commonly used technologies by businesses within the scope of digital transformation are big data analytics, artificial intelligence, blockchain, cloud computing, ERP systems, and robotic

process automation. These technologies enable faster recording of transactions, easier tracking of data, and greater transparency of financial information. For example, big data technologies make not only structured financial data but also unstructured data such as text, images, audio, and video usable for auditing purposes (Leng & Zhang, 2024).

From an auditing perspective, the digitalization of business processes is changing the nature of audit evidence. While in traditional auditing the auditor primarily evaluates documents, invoices, accounting records, and year-end reports; in digitized businesses, audit evidence is generated through system records, transaction logs, automated approval traces, database records, and digital control outputs. Therefore, the auditor should now evaluate not only the accuracy of financial transactions but also the reliability of the information systems in which these transactions are generated (Aditya et al., 2018).

Digitalization is also expanding the scope of auditing. The traditional sample-based audit approach is increasingly being replaced by more comprehensive methods that can analyze the entire data population. Thanks to big data analytics and AI-powered systems, auditors can analyze more transactions in a shorter time, identify unusual transaction patterns, and determine fraud risks at an earlier stage (Bani et al., 2025).

However, digitalization does not only create opportunities; it also generates new risks. Issues such as system complexity, data security, cyberattacks, access rights, algorithmic errors, data integrity, and the reliability of digital evidence have become critical from an auditing perspective. Therefore, auditing digital business processes requires knowledge of information technologies, data governance, and cybersecurity that goes beyond classical accounting auditing (Fang et al., 2025; Aditya et al., 2018).

2.2. Industry 4.0 and its Effects on Auditing

Industry 4.0 refers to a new production and management model in which automation, artificial intelligence, the Internet of Things, big data, cloud

computing, robotic systems, and cyber-physical structures are used together in businesses. In this model, business processes become more interconnected, faster, and more data-driven. From an auditing perspective, this means that the operational structure of the audited business becomes more complex.

In an Industry 4.0 environment, the auditor is no longer just someone who examines transaction documents; they must also understand how systems work, how data is generated, how controls are automated, and what algorithms decision-making mechanisms are based on. In particular, artificial intelligence and machine learning applications can support the auditor's professional judgment; however, they also raise issues of algorithmic transparency and explainability (Green et al., 2023).

Industry 4.0 technologies have the potential to improve audit quality. Artificial intelligence can be used in anomaly detection, big data analytics in the analysis of the entire transaction population, blockchain in the immutability of transaction records, and RPA in the automation of repetitive audit tasks. Thanks to these technologies, auditing becomes faster, more comprehensive, and more evidence-based (Manita et al., 2020; Bani et al., 2025).

Big data analytics enables auditors to work with large datasets instead of samples. This expands the scope of audits and allows for earlier detection of indicators of errors or fraud. Blockchain technology, on the other hand, increases transaction traceability by allowing transactions to be recorded in a timestamped and immutable manner (Bani et al., 2025; Leng & Zhang, 2024).

However, Industry 4.0 also creates significant competency challenges for auditors. Auditors need more than just knowledge of accounting, finance, and regulations. In the digital age, auditors must also be knowledgeable in data analytics, ERP structures, cybersecurity, cloud systems, automated controls, and the interpretation of artificial intelligence outputs. Otherwise, the auditor may be able to interpret the data generated by the technology; however, they may not be able to adequately assess whether this data is reliable (Aditya et al., 2018; Bani et al., 2025).

2.3. Cloud Systems and Remote Work

Cloud computing allows businesses to perform data storage, transaction execution, application use, and reporting processes through internet-based infrastructures instead of physical servers. This structure provides businesses with flexibility, scalability, cost advantages, and ease of remote access. From an auditing perspective, cloud systems enable auditors to access client company data without physically visiting the company (Bani et al., 2025).

Cloud systems have played a significant role in the development of remote auditing applications. Especially in the post-pandemic period, audit teams transmit document requests through online platforms, receive digital evidence through secure file-sharing systems, hold meetings online, and conduct some audit tests remotely. Ez-Zaidi and Ghandari's study indicates that digital tools are used in auditing firms, document sharing has shifted from the classic e-mail method to more advanced applications, and some audit tests can be performed entirely remotely (Ez-Zaidi & Ghandari, 2023).

The main advantages of remote auditing are cost savings, time efficiency, geographical flexibility, and easier collaboration for international audit teams. Auditors can now collect digital documents from clients in different countries or cities, conduct interviews online, and prepare audit files electronically. This makes the audit process more flexible (Bani et al., 2025; Ez-Zaidi & Ghandari, 2023).

However, cloud systems and remote work also carry significant audit risks. These include data security, confidentiality, unauthorized access, service provider dependency, integrity of digital evidence, and the reliability of documents obtained remotely. The country where data stored in the cloud is kept, who has access to it, and the security protocols used for protection are important from an audit perspective (Fang et al., 2025; Bani et al., 2025).

Another limitation of remote auditing is the reduction in face-to-face interaction. The auditor not only reviews documents but also observes, interviews employees, evaluates physical controls, and tries to understand the company environment. Remote monitoring can

create limitations in these areas. Therefore, the remote monitoring model should be supported by appropriate security protocols, verification mechanisms, and robust digital governance structures (Bani et al., 2025).

2.4. ERP Systems and Integrated Controls

ERP systems are enterprise information systems that bring together a business's accounting, finance, purchasing, sales, inventory, production, human resources, and reporting processes under a single integrated system. Thanks to ERP systems, business processes are interconnected, data duplication is reduced, transaction traceability is increased, and management can access more integrated information. Therefore, ERP systems have a central importance in terms of internal control and auditing in digitized businesses.

From an auditing perspective, the most important feature of ERP systems is the systematic and traceable recording of transactions. For example, in the purchasing process, the stages of request creation, supplier selection, approval, order, goods receipt, invoice recording, and payment can be carried out interconnectedly within the ERP system. This structure allows the auditor to evaluate control points from the beginning to the end of the process (Kagermann et al., 2008).

ERP systems include automated controls in addition to manual controls. Authorization limits, separation of duties, automatic approval flows, consistency checks, mandatory field checks, system alerts, and transaction logs are among these controls. An effectively designed ERP control structure can reduce the risk of erroneous transaction entries, unauthorized access, and irregular transactions. From an internal audit perspective, what matters is not only whether these controls are defined in the system, but whether they are actually functioning (Kagermann et al., 2008).

ERP systems also strengthen the link between information technology auditing and internal auditing. When evaluating the accuracy of financial data, the auditor should also analyze the system environment

in which this data was generated. User permissions, superuser access, separation of duties violations, batch-input processes, interface controls, data transfers, and system changes are critical areas in ERP auditing (Kagermann et al., 2008).

With digital transformation, ERP systems are becoming integrated with IoT, MES, and smart dashboards. This integration, especially in manufacturing businesses, increases process traceability and can reduce audit time. According to a systematic review by Bani et al., IoT, ERP, MES, and smart dashboard integrations strengthen traceability, increase compliance, and reduce audit time (Bani et al., 2025).

However, ERP systems are not without risks. Incorrectly configured permissions, inadequate separation of duties, incomplete log records, poor change management, data transfer errors, and system integration problems can lead to serious audit findings. Therefore, in ERP audits, not only transaction accuracy but also system design, control logic, user roles, and data flows should be evaluated together (Aditya et al., 2018; Kagermann et al., 2008).

2.5. Emerging Digital Risks

While digital transformation provides businesses with speed, transparency, efficiency, and comprehensive analysis capabilities, it also generates new risk categories. These risks go beyond classic financial errors or lack of control; they encompass areas such as cybersecurity, data integrity, algorithmic decision-making, system dependency, technology provider risk, lack of regulation, and the reliability of digital evidence (Fang et al., 2025; Bani et al., 2025).

Digital transformation has introduced a set of emerging risks that extend beyond the traditional boundaries of financial control and operational compliance. As organizations increasingly rely on interconnected systems, cloud-based infrastructures, mobile applications, automated workflows, and external digital interfaces, the internal audit function is required to evaluate not only the efficiency of digital processes but also the vulnerabilities created by these technologies. In this context, digital risks directly influence the reliability of financial

reporting, the integrity of audit evidence, the effectiveness of internal controls, and the overall resilience of the organization.

Cybersecurity and data privacy constitute one of the most critical risk areas in digitally transformed organizations. Business data is now generated, processed, stored, and transferred across multiple platforms, including enterprise systems, cloud environments, mobile applications, and third-party connections. This interconnected structure increases exposure to unauthorized access, data leakage, malware attacks, service interruptions, and other forms of cyber disruption. From an audit perspective, such risks are significant because they may compromise the reliability of financial information and weaken the evidential basis on which audit conclusions are formed (Aditya et al., 2018; Fang et al., 2025).

A further risk area relates to system complexity and integration. Digital transformation often requires organizations to connect legacy systems with newly adopted technologies. However, differences in system architecture, data formats, process logic, and user capabilities may generate operational uncertainty. Weak integration between old and new systems can create inconsistencies in data flows, reduce process transparency, and increase the need for additional audit procedures. As a result, auditors may be required to obtain broader evidence, perform more detailed system evaluations, and reassess the reliability of information produced within digitally integrated environments (Leng & Zhang, 2024).

Algorithmic opacity has also become an important concern for internal auditors. Artificial intelligence-supported audit tools can identify unusual transactions, assign risk scores, and classify specific activities as suspicious. Nevertheless, the logic behind these classifications may not always be sufficiently transparent. This creates challenges for explainability, professional judgment, audit documentation, and accountability. Although advanced digital tools can increase the speed and scope of audit procedures, they may also introduce new difficulties when auditors cannot clearly determine why a system has treated a particular transaction as risky (Green et al., 2023).

Digitalization also changes the temporal and structural nature of audit evidence. In traditional audit environments, evidence is generally collected and evaluated at specific points in time, often after the completion of a reporting period. In contrast, continuous audit environments generate evidence through real-time or near-real-time data flows. Therefore, audit findings are no longer limited to static conclusions derived from periodic reviews; they may instead emerge from constantly updated system-based assessments. This transformation requires auditors to reconsider how evidence is collected, evaluated, documented, and reported in dynamic digital environments (Green et al., 2023; Sadek et al., 2024).

Human resource and competency-related risks represent another major challenge in digital auditing. The effectiveness of digital audit tools depends not only on the technical quality of the systems used, but also on the auditor's ability to understand, interpret, and critically evaluate their outputs. Limited digital literacy, resistance to technological change, insufficient training, and the misinterpretation of system-generated results may reduce the effectiveness of digital audit practices. Therefore, the successful use of digital audit technologies requires continuous professional development, stronger technological competence, and the integration of professional skepticism with analytical and digital skills (Farhan & Kawther, 2023; Bani et al., 2025).

Consequently, digital risks are expanding the scope of internal audit and demanding a more integrated perspective from the auditor. The auditor should now evaluate not only financial records but also systems, algorithms, data flows, access rights, cloud infrastructure, automated controls, and the reliability of digital evidence together. Therefore, in the digital age, internal audit is being repositioned as a strategic assurance function that is technology-supported but based on human judgment.

Chapter Summary

This chapter examines the impact of digital transformation on business processes and the audit environment. With digitalization, the nature of audit evidence has changed; system records, transaction logs,

automated approval trails, and digital control outputs have become more important in the audit process.

The chapter also evaluates the contributions of Industry 4.0 technologies, cloud systems, remote work, and ERP systems to auditing. Furthermore, it emphasizes that risks such as cybersecurity, data confidentiality, algorithmic opacity, system integration, and lack of digital competence create new responsibilities for internal auditing.

In conclusion, in the digital age, internal auditing is transforming from an activity that merely examines financial records into a strategic assurance function that evaluates systems, data, automated controls, and digital risks together.

Chapter 3 – Audit Methodology in the Digital Age

Introduction

In the digital age, audit methodology is moving away from the traditional understanding of document review and periodic control, transforming into a risk-oriented, data-driven, and continuously updated structure. The increasing reliance of businesses on digital systems, ERP infrastructures, cloud-based applications, artificial intelligence tools, and big data analytics directly affects the planning, evidence gathering, analysis, monitoring, and reporting phases of the audit process.

This chapter addresses the fundamental elements of audit methodology in the digital age. First, risk-based audit planning is explained; then, digital audit evidence, data-driven audit, continuous audit, and continuous monitoring practices, as well as digital working papers, are evaluated. The aim of the chapter is to reveal how digitalization is transforming audit methods and what methodological approaches internal auditors need in this new environment.

3.1. Risk-Based Audit Planning

Audit planning is one of the most critical areas of transformation in audit methodology in the digital age. While planning in the traditional audit approach is mostly shaped by the annual audit calendar, standard audit programs, and past period findings; digitalization has transformed the planning process into a more dynamic, data-driven, and continuously updated structure. In the digital economy, businesses' business processes, product and service delivery methods are being restructured through technology; this makes businesses more agile, efficient, and competitive, while also making it necessary for the audit

function to become more flexible, transparent, and analytical (Daidj, 2022; Guliyeva & Gaziyeva, 2025; Betti & Sarens, 2021).

Audit planning is a strategic stage carried out at the beginning of the audit process and aims to give sufficient attention to critical areas, identify potential problems in a timely manner, and use audit resources effectively. In international audit standards, planning is also considered as the creation and documentation of the overall strategy that determines the scope, timing, and direction of the audit. At this stage, the company's activities, industry conditions, internal control system, reporting obligations, materiality level, and potential risk areas are taken into consideration (Guliyeva & Gaziyeva, 2025; Fang et al., 2025).

The risk-based auditing approach forms the theoretical basis of audit planning in the digital age. According to this approach, the audit plan should be created taking into account the company's risk universe, and audit resources should be directed to the areas with the highest risk. Therefore, before preparing the annual audit plan, the institution's risk records, risk map, and existing control weaknesses should be analyzed in detail. Areas with a high risk level are subjected to more frequent, or even continuous, audits when necessary; while relatively low-risk areas can be audited less frequently. This approach ensures that audit needs are met systematically and proportionally to the risk level (Guliyeva & Gaziyeva, 2025; Stepanyan, 2023; Kabuye et al., 2017).

Digitalization has transformed risk-focused planning from a purely annual activity into a continuous risk assessment and planning mechanism. While traditional audit plans are usually prepared at the beginning of the year and implemented with limited changes throughout the year, the risk profile changes much faster in digitized businesses. The initiation of a new digital project, a major update to the ERP system, a cybersecurity breach, a sudden increase in sales volume, an unexpected change in the cost structure, or the detection of internal control weaknesses may necessitate a revision of the audit plan. Therefore, in contemporary internal audit functions, the audit plan has acquired the character of a "living document" (Betti & Sarens, 2021; Stepanyan, 2023; Ahmed & Japee, 2025).

The fundamental difference in risk-focused planning in the digital age is that planning decisions are based not only on management opinions or past audit findings, but also on big data analysis, risk indicators, and system-based alerts. Advanced internal audit units create risk dashboards by monitoring operational and financial metrics in real time; and redefine audit priorities when anomalies are detected. For example, an unusual increase in returns for a specific product group, irregularities in supplier payments, sudden changes in access rights, or an increase in manual entries outside the system may lead to the addition of a new task to the audit plan (Ahmed & Japee, 2025; Ayoub et al., 2025; Lotfy, 2026).

This transformation has also brought the agile audit approach to the forefront. Agile audit refers to conducting audit activities with short cycles, prioritized task lists, and rapid feedback mechanisms. Instead of traditional annual plans, monthly or quarterly updated plans, audit backlog lists, and short audit sprints can be used. Thus, the audit function can respond to the rapidly changing risk environment in a shorter time. This approach is based on the understanding that "today's risk should not wait for tomorrow" (Stepanyan, 2023; Daidj, 2022).

Digitalization has also increased the possibilities of robotic process automation and analytical reporting in the planning phase. Auditors can now identify which accounts, units, or processes are showing unusual activity in the planning phase by analyzing large datasets. Some sources state that thanks to digital innovations, audit process flows and documentation can be automatically updated, strategic analysis reports can be generated during the planning phase, and routine tasks such as data collection, process mapping, and preliminary reporting can be supported by RPA (Ahmed & Japee, 2025; Stepanyan, 2023; Ishaku et al., 2023).

Another dimension of risk-focused digital planning is auditor competencies. In the digital environment, the scope of the internal audit function is not limited solely to financial controls; it also includes areas such as information technologies, cybersecurity, data privacy, algorithmic decision systems, cloud-based applications, and digital business models. Betti and Sarens' study indicates that digitalization

affects the internal audit function in three ways: the scope of audits is expanding, the need for agility and digital information in audit planning is increasing, and IT risks, and especially cybersecurity threats, are gaining more importance (Betti & Sarens, 2021). In this context, risk-focused planning in the digital age seeks answers not only to the question of "which processes will be audited?" but also to the question of "which digital risks threaten the strategic objectives of the company?" (Fang et al., 2025; Saat et al., 2025).

In conclusion, risk-based auditing planning in the digital age is transforming from a static and periodic process into a dynamic, data-driven, continuously updated, and technology-integrated methodology. In this methodology, the audit function must allocate its limited resources to high-risk areas while simultaneously holistically evaluating the company's digital transformation strategy, cyber resilience, data governance, and control environment (Daidj, 2022; Betti & Sarens, 2021; Guliyeva & Gaziyeva, 2025).

3.2. Digital Audit Evidence

Audit evidence is the body of information and documents that support the conclusions reached by the auditor. In the digital age, the nature of audit evidence has changed significantly. While in the traditional audit environment evidence is mostly obtained through physical documents, signed forms, written approvals, accounting vouchers, and records examined through sampling; in the digital environment, evidence is obtained from sources such as ERP systems, cloud-based accounting software, transaction logs, access logs, system alerts, electronic approval flows, database outputs, e-mail traces, digital working papers, and automated control reports (Guliyeva & Gaziyeva, 2025; Saat et al., 2025; Ahmed & Japee, 2025).

This transformation has both broadened the scope of audit evidence and made it more complex to assess its reliability. The reliability of digital evidence depends not only on the content of the document, but also on the system from which the data was generated, who has access to the system, whether data changes are traceable, whether

authorization matrices function correctly, and whether data integrity is maintained. Therefore, in the digital age, the auditor should evaluate not only the accuracy of the accounting record but also the reliability of the information system that produced that record (Lotfy, 2026; Ayoub et al., 2025; Ishaku et al., 2023).

The widespread adoption of ERP systems provides significant opportunities for digital audit evidence. Because ERP systems consolidate a company's financial transactions on a single platform, auditors can directly access large datasets, perform automated audit tests, and conduct full population tests instead of sampling. Audit software such as IDEA, CaseWare, and ACL can analyze large financial datasets from ERP and other digital sources to identify anomalies and risk indicators (Guliyeva & Gaziyeva, 2025; Ahmed & Japee, 2025). This development leads to a significant improvement in the quality of audit evidence. In sample-based auditing, the auditor relies on the assumption that the selected samples represent the population. However, digital tools allow for testing the entire transaction population whenever possible. This reduces sampling risk and increases the probability of detecting indicators of error or fraud. Digital audit evidence can be used not only for verifying past transactions but also for anomaly detection and early identification of risks (Ahmed & Japee, 2025; Lotfy, 2026; Kabuye et al., 2017).

Although digital evidence enhances the scope and efficiency of audit procedures, it also gives rise to specific risks concerning reliability, confidentiality, and regulatory compliance. Data integrity represents a primary concern, particularly when system records are susceptible to alteration, audit logs may be deleted, or user authorization controls are inadequately designed. Under such conditions, the credibility and auditability of digital evidence may be significantly compromised. Moreover, the use of datasets containing personal data, commercially sensitive information, or confidential financial records requires strict attention to data privacy and confidentiality. Access to such information should be limited through appropriate authorization protocols and supported by secure data transmission processes. In cloud-based systems, further consideration should be given to the physical location of data storage, the applicable data protection framework,

and the adequacy of the cloud service provider's security controls (Saat et al., 2025; Ahmed & Japee, 2025; Ayoub et al., 2025).

Digitalization has also changed the timing of audit evidence. While evidence in traditional audits is mostly collected after the period, digital systems allow for the production of evidence in real-time or near real-time. Continuous auditing and continuous monitoring practices make it possible to collect audit evidence not only retrospectively but also simultaneously. As highlighted by ISACA, continuous auditing and monitoring practices in the digital transformation environment support the timely monitoring of risks and the real-time collection of audit evidence (Guliyeva & Gaziyeva, 2025; Stepanyan, 2023).

Artificial intelligence and machine learning tools are also used in the evaluation of digital audit evidence. These tools can identify hidden patterns, unusual transactions, and high-risk records within large datasets. However, AI outputs alone should not be considered as the final audit evidence. The auditor should evaluate algorithmic results within the framework of professional skepticism, considering the model's data source, assumptions, explainability, and margin of error. XAI-focused studies also emphasize that traditional black-box AI systems pose problems in the audit context; it is necessary for auditors not only to reach the correct conclusion but also to justify this conclusion to regulatory authorities, clients, and other stakeholders (Lotfy, 2026; Ahmed & Japee, 2025).

Explainable AI makes a significant contribution to the interpretation of digital audit evidence. XAI strengthens the transparency, traceability, accountability, and auditability features of algorithmic decisions. Especially when analyzing cybersecurity risks, fraud indicators, or complex transaction flows, the auditor's ability to interpret the results generated by AI is crucial.

It is necessary to understand why the generated risk score was formed. This shows that digital evidence is not merely a technical output, but an element of evaluation integrated into professional judgment (Lotfy, 2026).

In digital audit environments, the strength of audit evidence depends on a chain of reliability that extends from data generation to audit interpretation. Evidence obtained from digital systems should therefore be evaluated in relation to the credibility and security of its source, the controls embedded in the system from which it is extracted, and the integrity of the processes through which it is analyzed. The analytical techniques and technological tools used by the auditor should also be assessed, since inappropriate processing methods may weaken the reliability of otherwise relevant data. Equally important is the auditor's role in interpreting digital outputs through professional judgment and documenting the rationale behind the conclusions reached. Accordingly, the mere availability of data is insufficient for audit purposes. Digital evidence can support robust audit conclusions only when it is reliable, complete, traceable, explainable, and verifiable within an auditable control framework (Lotfy, 2026; Ahmed & Japee, 2025; Eklöv Alander & Holmgren Caicedo, 2026).

3.3. Data-Driven Auditing

Data-driven auditing is one of the most significant areas of transformation in audit methodology in the digital age. While the traditional audit approach largely relies on sampling, manual document review, and periodic control tests; data-driven auditing refers to a more comprehensive audit approach conducted with the analysis of large datasets, full population tests, anomaly detection, process mining, AI-assisted risk scoring, and visualization tools (Ahmed & Japee, 2025; Betti & Sarens, 2021; Ayoub et al., 2025).

With digitalization, the volume of data produced by businesses has rapidly increased. Betti and Sarens state that the volume of digital content is growing very rapidly on a global scale and that businesses are restructuring their strategies to adapt to this new digital business environment (Betti & Sarens, 2021). This transformation has expanded the methodological scope of internal audit. The function is now expected to move beyond limited document-based testing and

develop the capacity to analyze large datasets, evaluate risks arising from digital systems, and provide assurance through technology-supported audit methods (Daidj, 2022; Ishaku et al., 2023).

One of the most important contributions of data-driven auditing is full population testing. In traditional auditing, auditors select a sample from the transaction universe due to time and resource constraints. However, thanks to ERP systems, data analytics software, and automated testing tools, the entire transaction universe can be analyzed. This method reduces the risk of traditional sampling and increases the probability of detecting unusual transactions. In the context of digital transformation, the fact that ERP systems aggregate financial transactions on a single platform offers auditors the opportunity to directly extract and analyze large datasets; thanks to automated tests and full population analyses, indicators of errors and fraud can be detected more effectively (Guliyeva & Gaziyeva, 2025; Ahmed & Japee, 2025; Lotfy, 2026).

Data analytics not only allows auditors to verify transactions but also enables them to prioritize risks and more accurately define the scope of the audit. For example, different suppliers with the same IBAN in supplier payments, unusual entries made on weekends or outside working hours, transaction changes made by unauthorized users, rounded-amount payments, subprime split purchases, or unexpected inventory movements can be identified using data analytics. Such analyses direct the auditor's attention to high-risk transaction clusters (Ahmed & Japee, 2025; Ayoub et al., 2025; Kabuye et al., 2017).

Artificial intelligence and machine learning are taking data-driven auditing to a more advanced stage. AI can identify patterns and relationships in large datasets that are difficult for the human eye to detect. Furthermore, risk prediction models can be developed using past events, transaction characteristics, and control results. In the digital audit literature, it is stated that artificial intelligence and advanced data analytics transform auditing from retrospective verification to continuous and predictive assurance. Auditing is no longer limited to checking whether past transactions have been correctly recorded; it has gained the function of anticipating emerging risks, detecting real-time

anomalies, and generating proactive intervention recommendations (Lotfy, 2026; Ahmed & Japee, 2025; Ishaku et al., 2023).

Another dimension of data-driven auditing is process mining. Process mining reveals the actual process flow by analyzing the transaction steps recorded in the company's information systems. Thus, the differences between the process defined in written procedures and the process actually implemented can be seen. For example, whether approval steps were skipped in the purchasing process, whether pre-payment goods receipt control was performed, or whether authorization limits were exceeded can be analyzed with process mining. This method contributes to identifying gaps between control design and control implementation (Guliyeva & Gaziyeva, 2025; Daidj, 2022).

Data-driven auditing also improves audit quality. A systematic literature review indicates that advanced data analytics improves the accuracy, reliability, and timeliness of audit results through full population testing, real-time monitoring, and anomaly detection (Ahmed & Japee, 2025). This finding demonstrates that data-driven auditing is not merely the use of a technological tool, but a structural transformation of the audit methodology that enhances its assurance level. However, data-driven auditing also has some limitations. The reliability of digital audit procedures is closely linked to the condition of the datasets on which they are based. When data is incomplete, inaccurate, inconsistent, or collected in different formats, analytical procedures may produce results that do not accurately reflect the underlying transactions or risks. In AI-assisted audit processes, another important concern is the possibility that models may reproduce or amplify weaknesses embedded in historical data. For example, models trained on biased, incomplete, or incorrectly classified data may generate distorted risk assessments and lead to misleading audit interpretations. These risks indicate that auditors should not rely on digital outputs mechanically. Instead, they need sufficient competence in data analytics, statistics, information systems, and cybersecurity to question, validate, and interpret technology-based audit evidence within the specific context of the audit engagement.

The study findings indicate that in the digital age, auditors need technical competencies in artificial intelligence, analytics, and cybersecurity in addition to traditional audit knowledge; they also need skills such as ethical reasoning, communication, and compliance (Ahmed & Japee, 2025; Ayoub et al., 2025; Saat et al., 2025).

In data-driven auditing, professional skepticism becomes even more important. The auditor should not mechanically accept the results produced by analytical tools; they should evaluate the data source, model assumptions, exception criteria, and the meaning of the analysis results in the company context. The XAI approach gains importance at this point. Explainable artificial intelligence helps the auditor integrate the AI output with professional reasoning by showing why algorithmic risk scores are generated (Lotfy, 2026; Eklöv Alander & Holmgren Caicedo, 2026).

In this context, data-driven auditing moves the audit function to a more proactive, analytical, and strategic structure in the digital age. However, for this transformation to be healthy, data governance, system access controls, model validation, ethical use principles, and auditor competencies must be considered together. Otherwise, data-driven auditing may risk generating false assurances instead of improving audit quality (Lotfy, 2026; Ahmed & Japee, 2025; Fang et al., 2025).

3.4. Continuous Auditing and Continuous Monitoring

Continuous auditing and continuous monitoring refer to the evolution of audit methodology from a periodic structure to a real-time structure in the digital age. While controls and processes are examined at the end of specific periods in traditional auditing, digital systems allow transaction data, control indicators, and risk signals to be analyzed simultaneously or at short intervals. This change enables the audit function to work proactively rather than reactively (Guliyeva & Gaziyeva, 2025; Stepanyan, 2023; Ahmed & Japee, 2025).

With digital transformation, traditional end-of-period audits have become insufficient. Transaction volumes have increased in businesses,

processes have become automated, data flows have accelerated, and cyber risks can have an immediate impact. Therefore, audits conducted only at the end of the year may not be sufficient to detect risks in a timely manner. Since digital systems enable real-time data analysis, businesses can detect risks earlier and take necessary precautions faster. It is stated that significant risks can grow unnoticed and lead to serious problems if continuous monitoring is not carried out (Guliyeva & Gaziyeva, 2025; Lotfy, 2026).

Continuous auditing refers to the systematic application of audit procedures at specific intervals or with automated triggers. Continuous monitoring, on the other hand, is the regular monitoring of process performance, control indicators, and risk signals by management and controllers. From an internal audit perspective, these two concepts complement each other. While management monitors the functioning of controls through continuous monitoring, internal auditing evaluates the effectiveness and reliability of these monitoring mechanisms through continuous auditing (Stepanyan, 2023; Ahmed & Japee, 2025; Daidj, 2022).

Risk indicators, control indicators, and automated alert mechanisms are at the core of continuous auditing practices. For example, exceeding authorization limits, high-value manual entries, duplicate payments, unusual user access, unexpected decreases in stock levels, increases in canceled sales invoices, or off-system correction entries can generate automated alerts. These alerts enable the audit function to initiate a rapid review of the relevant transaction or process (Ahmed & Japee, 2025; Stepanyan, 2023; Ayoub et al., 2025).

Stepanyan's study states that the digitally prioritized internal audit function uses agile internal audit and continuous audit methodologies; data correlation and real-time big data analytics make internal audit functions more proactive in identifying potential control failures (Stepanyan, 2023). In this approach, past events, operational losses, near misses, and current control indicators are evaluated together to generate predictions about the probability of the risk occurring in the future. One of the important advantages of continuous audit is that it increases the timeliness of audit findings. While a control failure

may be detected months later in traditional auditing, the same failure can be detected quickly in a continuous audit system. This is particularly critical in risks such as financial loss, fraud, cyber attack, or non-compliance with regulations. In digital twin and XAI-based audit approaches, real-time assurance, continuous monitoring, predictive risk simulation, and interpretable decision support are also prominent (Lotfy, 2026; Ishaku et al., 2023).

Continuous auditing is also important in terms of cybersecurity assurance. In digitized businesses, data integrity, system continuity, access security, and algorithmic transaction reliability are key risk areas. In XAI-supported digital twin audit frameworks, cyberattack scenarios can be simulated to evaluate the effectiveness of controls, data integrity, and their impact on audit risk. Such approaches allow the auditor not only to examine past events but also to assess the impact of potential attack or disruption scenarios in advance (Lotfy, 2026; Saat et al., 2025).

Continuous auditing and monitoring practices also change the reporting approach. While traditional audit reports are mostly prepared in specific periods and as long documents, dynamic dashboards, risk scores, automated alerts, and visual reports are used more frequently in the digital age. Stepanyan states that in digitally-first businesses, hundreds of pages of physical reports are not compatible with the core values of the digital age; instead, dynamic continuous reporting methods with escalation based on the severity of events and risk dashboards prepared with visualization tools such as Tableau or Power BI can be used (Stepanyan, 2023).

However, continuous auditing does not mean that all audits should become fully automated. The auditor's professional judgment, ability to assess the control environment, and ability to interpret findings within the company context are still central. Automated systems can generate risk signals; however, the auditor should assess whether this signal points to a genuine control deficiency, system error, indication of fraud, or a change in routine business practices (Lotfy, 2026; Ahmed & Japee, 2025; Eklöv Alander & Holmgren Caicedo, 2026).

There are certain prerequisites for establishing continuous audit and monitoring systems. These include a reliable data infrastructure, ERP or similar integrated systems, clear authorization matrices, regular logging, data quality controls, accurate design of risk indicators, audit analytics tools, and a qualified auditor staff. In addition, risks such as data privacy, unauthorized monitoring, algorithmic bias, and false alarm generation should also be considered in continuous audit systems (Ahmed & Japee, 2025; Saat et al., 2025; Ayoub et al., 2025).

In conclusion, continuous audit and continuous monitoring transform the internal audit function from a periodic control mechanism to a strategic structure that provides continuous assurance in the digital age. This approach supports early detection of risks, rapid remediation of control deficiencies, real-time collection of audit evidence, and more timely decision-making by management. However, an effective continuous audit system depends on a balanced integration of technology and professional judgment (Stepanyan, 2023; Lotfy, 2026; Betti & Sarens, 2021).

3.5. Digital Working Papers and Documentation

The final important dimension of audit methodology in the digital age is the working paper and documentation process. Working papers are fundamental tools that document the auditor's work, collected evidence, applied procedures, conclusions reached, and professional judgment. While in traditional auditing, working papers mostly consist of physical files, manual checklists, and separately stored documents; in a digital audit environment, working papers are created integrated with electronic platforms, cloud-based file systems, audit management software, automated referencing, digital signatures, data links, and dashboards (Stepanyan, 2023; Guliyeva & Gaziyeva, 2025; Daidj, 2022).

One of the most important contributions of digital working papers is traceability. In the audit process, it can be recorded on the system which procedure was applied by whom, when, using which data source, and with what result. This is important for both quality

assurance reviews and post-audit review processes. Furthermore, digital working papers allow for the comparison of current period analyses with previous period audit findings, monitoring of control vulnerabilities, and tracking of action plans (Stepanyan, 2023; Lotfy, 2026; Ahmed & Japee, 2025).

Digital documentation increases audit efficiency. Routine data collection, updating process flows, preparation of preliminary analysis reports, and completion of standard working paper sections can be automated. The added resources state that thanks to digital innovations, audit process flows and documentation can be automatically updated, strategic analysis reports can be automatically generated during the planning phase, and technologies such as RPA can perform routine planning tasks such as data collection, process mapping, and preliminary report preparation (Ahmed & Japee, 2025; Stepanyan, 2023; Ishaku et al., 2023).

Digital working papers also facilitate teamwork. Especially in remote audits, multi-location audits, and international group audits, cloud-based working environments allow audit teams to work simultaneously on the same files. Auditors can share electronic documents, conduct interviews online, and record comments and review notes on the system. Digital planning resources state that cloud technologies offer auditors secure remote access to the audited entity's databases, electronic document sharing, and video conferencing capabilities; this reduces audit costs and time while increasing continuous monitoring capacity (Guliyeva & Gaziyeva, 2025; Saat et al., 2025; Betti & Sarens, 2021).

The use of digital working papers creates important control obligations in relation to access management, document integrity, and information security. Since audit documentation may include confidential financial records, operational data, and other sensitive organizational information, access rights should be restricted according to clearly defined roles and responsibilities. This ensures that audit personnel can access only those files that fall within the scope of their assigned duties. Moreover, version control mechanisms are necessary to maintain the reliability and audit trail of working papers. Revisions

should be systematically logged by identifying the user who made the change, the date of modification, and the nature of the update. From an information security perspective, digital working paper systems should also incorporate safeguards such as encryption, secure backups, multi-factor authentication, and secure data transfer protocols to reduce the risk of unauthorized access, data loss, or information leakage (Saat et al., 2025; Ahmed & Japee, 2025; Ayoub et al., 2025).

Another dimension of digital documentation is dynamic reporting. While findings in traditional audit files are often reported at the end of the period, digital platforms allow for real-time monitoring of the status of the finding, the level of risk, the responsible unit, the target date, and the status of the action. Stepanyan's study states that in digitally prioritized internal audit functions, dynamic continuous reporting methods with escalation based on importance should be adopted instead of physical and lengthy reports; and that visualizing clear findings and risk levels with tools such as Tableau or Power BI is consistent with the digitalization journey of internal audit (Stepanyan, 2023).

Agile audit methodologies also strengthen the use of digital working papers. Through Scrum or Kanban boards, the stages of the audit task, those responsible, the completion status, and pending tasks can be tracked. Thus, audit progress can be seen not only by the audit team but also by management and audited entities at the appropriate level of authority. This approach increases transparency, communication, and accountability in the audit process. Stepanyan notes that Scrum/Kanban dashboards provide a unified view of audit progress and enable greater participation of audited parties in the process (Stepanyan, 2023; Eklöv Alander & Holmgren Caicedo, 2026).

Digital working papers are also important in terms of audit quality. Standardized templates, automated checklists, mandatory fields, electronically controlled documents are important. Digital approval flows and quality review notes enhance the completeness of the audit file. However, digital documentation should not only serve the function of document storage. A good digital working paper should clearly show the procedure followed by the auditor, the data source used, the

findings reached, the risk assessed, and the conclusion reached. In other words, digitalization does not automatically make weak documentation strong; it only improves audit quality when combined with a well-designed methodology (Stepanyan, 2023; Ahmed & Japee, 2025; Daidj, 2022).

At this point, the principles of explainability and auditability are particularly important. When artificial intelligence, data analytics, or automated control tests are used, working papers should document not only the results but also the model used, the dataset, the filtering criteria, the exception rules, and how the auditor evaluated these results. The XAI approach emphasizes that algorithmic outputs should be transparent, traceable, accountable, and auditable (Lotfy, 2026). This principle demonstrates that digital working papers are not merely a place to store technical outputs, but a fundamental evidence space where audit reasoning is documented. Consequently, digital working papers and documentation are not a complementary but a central element in the digital transformation of audit methodology. All processes, from audit planning to evidence gathering, data analysis to continuous monitoring, findings tracking to reporting, are supported by digital documentation. An effective digital documentation system should be traceable, secure, standardized, dynamic, explainable, and support audit quality (Stepanyan, 2023; Lotfy, 2026; Ahmed & Japee, 2025).

Chapter Summary

This section discusses the transformation of audit methodology in the digital age. It emphasizes that the traditional approach of document review and periodic checks has been replaced by a risk-focused, data-driven, continuous, and technology-integrated audit approach. It explains that risk-based auditing planning is no longer based solely on static annual plans, but on continuously updated risk indicators and data analytics.

The section also evaluates digital audit evidence, data-driven auditing, continuous auditing, continuous monitoring, and digital working

papers. It notes that digital audit evidence consists more of system records, transaction logs, electronic approval flows, and database outputs than physical documents. It states that data-driven auditing enables full population analysis instead of sampling, anomaly detection, and AI-assisted risk assessment.

It highlights that continuous auditing and continuous monitoring practices transform the audit function from a retrospective control mechanism to a strategic structure providing real-time assurance. Finally, it explains that digital working papers and documentation contribute to the traceable, secure, explainable, and auditable conduct of the audit process.

In conclusion, this section demonstrates that the fundamental aim of audit methodology in the digital age is not to replace the auditor's professional judgment with technology, but to use it in a way that makes the audit process faster, more evidence-based, continuous, and strategic. Therefore, a successful digital audit approach must consider the use of technology together with the auditor's professional skepticism, ethical considerations, and analytical thinking skills.

PART II

DIGITAL RISKS, CONTROLS AND TECHNOLOGIES

Chapter 4 – Internal Control Systems in Digital Organizations

Introduction

In digital organizations, internal control systems are evolving beyond the traditional manual control approach into a technology-supported, data-driven, and continuously monitorable structure. ERP systems, automated controls, AI-powered analytics, digital approval workflows, and real-time monitoring mechanisms are making the control environment of businesses more dynamic and integrated.

This section examines the internal control structure in digital organizations based on the COSO framework; it explains automated controls, preventive and detective controls, and the separation of duties in ERP systems. The aim of this section is to evaluate how digitalization is transforming internal control systems and what new control areas it is creating from an internal audit perspective.

4.1. COSO Framework in Digital Organizations

In digital organizations, internal control systems have expanded beyond their traditional focus on the accuracy of financial transactions and have become an integrated governance mechanism that supports operational efficiency, data security, regulatory compliance, cyber risk management, real-time monitoring, and managerial decision-making. Within this transformation, the COSO framework remains a central reference model for designing and evaluating internal control systems. COSO conceptualizes internal control as a process that provides reasonable assurance regarding the achievement of operational, reporting, and compliance objectives, and organizes this process around five interrelated components: control environment, risk assessment, control activities, information and communication, and monitoring activities (Batte, 2025; Huang, 2026). The related literature

also indicates that COSO offers a flexible structure for evaluating internal control systems in technology-intensive environments, particularly in processes shaped by ERP systems, artificial intelligence, automation, and information technologies.

The control environment forms the foundation of internal control in digital organizations because it reflects organizational culture, ethical values, management's control awareness, accountability, and commitment to responsible governance before technological tools are considered. Even the most advanced ERP systems, artificial intelligence applications, or automated workflows cannot provide sufficient assurance if they operate within a weak control environment. Issues such as access rights, segregation of duties, approval mechanisms, and the monitoring of control exceptions ultimately depend on management's attitude toward control and the organization's accountability culture. Batte emphasizes that the control environment, through the "tone at the top," shapes ethical values, personnel competence, and management's operating style, thereby supporting operational, reporting, and compliance objectives (Batte, 2025). Espinosa-Jaramillo similarly highlights the importance of organizational culture and ethical orientation in the functioning of internal control systems in digital settings (Espinosa-Jaramillo, 2024).

Risk assessment has also become more dynamic as organizations increasingly rely on digital systems and real-time data. In traditional structures, risk assessment is often based on periodic reviews, previous audit findings, and managerial experience. In digital organizations, however, risks can be evaluated through transaction data, user behavior, system logs, real-time records, and external environmental indicators. This changes risk assessment from a static identification exercise into a continuous and data-supported process. Mo argues that digital transformation affects internal control quality through the COSO components by automating risk assessment, making control activities more intelligent, increasing transparency in monitoring, and strengthening information sharing (Mo, 2023). In this respect, risk assessment in digital organizations involves not only identifying risks but also monitoring them algorithmically, linking them to early warning mechanisms, and using risk indicators to inform control design.

Control activities represent one of the areas where the impact of digitalization is most visible. Approvals, authorizations, reconciliations, segregation of duties controls, access restrictions, transaction limits, exception reports, system validations, and automated alerts are all examples of control activities that can be embedded into digital systems. In contemporary organizations, these controls are increasingly performed through system rules, automated workflows, and ERP-based control points rather than through manual procedures alone. Batte states that control activities support the implementation of management directives through policies and procedures such as approvals, verifications, reconciliations, and segregation of duties. In modern control environments, tools such as blockchain, automated workflows, and system-based approval mechanisms can strengthen the real-time operation of these controls (Batte, 2025). However, the existence of automated controls does not by itself guarantee effectiveness; the control logic must be properly designed, aligned with relevant risks, and periodically reviewed.

The information and communication component has also gained broader significance in digital organizations. It no longer refers only to formal reporting, but also to the timely, accurate, accessible, reliable, and relevant transmission of information to appropriate users. ERP systems, data warehouses, automated dashboards, reporting tools, and control panels support management's decision-making processes while also facilitating the early identification of control deficiencies. Batte notes that ERP systems and automated dashboards improve organizational communication and enable data-driven decision-making (Batte, 2025). Accordingly, information and communication in digital internal control systems include not only the production of reports but also the communication of control exceptions, the dissemination of control awareness, and the capacity of management to respond quickly to emerging issues.

Monitoring activities have become more effective with the development of continuous monitoring and continuous auditing approaches. In traditional control structures, monitoring is often associated with periodic internal audit reviews or management evaluations. In digital organizations, however, transaction data, user activities, authorization changes, system errors, and unusual transaction patterns can be

monitored on an ongoing basis. Digital monitoring tools can identify control weaknesses, generate exception reports, and send automatic notifications to responsible managers, thereby supporting timely corrective action. Batte states that AI-powered monitoring tools can continuously evaluate control effectiveness and produce real-time anomaly alerts (Batte, 2025). This indicates that monitoring in digital organizations should not be limited to the existence of system-generated records; it should also involve the systematic analysis of these records and their integration into corrective and preventive control actions.

Overall, the COSO framework remains highly relevant in digital organizations because it allows internal control to be evaluated as a multidimensional governance system rather than as a narrow set of financial controls. The effectiveness of internal control in digital environments depends on the interaction between ethical culture, dynamic risk assessment, properly designed automated controls, reliable information flows, and continuous monitoring. Therefore, digitalization should not be viewed as a substitute for internal control. Instead, it should be understood as a factor that changes how internal controls are designed, operated, tested, and improved.

Therefore, in digital organizations, the COSO framework should be considered not as a static checklist, but as a dynamic internal control architecture that combines technological infrastructure with governance principles. Huang's work on the artificial intelligence industry also shows that the COSO components do not work independently but interact with each other; in particular, the relationship between the control environment, information and communication, risk assessment, and monitoring activities is decisive for internal control effectiveness (Huang, 2026).

4.2. Automated Controls

Automated controls are one of the most critical elements of internal control systems in digital organizations. These controls refer to verification, limitation, approval, matching, warning, record keeping, and

reporting mechanisms performed by the system without the need for manual human intervention. The main purpose of automated controls is to reduce the risk of errors and fraud, increase transaction reliability, standardize control practices, and provide management with access to real-time information.

Digitalization has moved internal control systems from manual and paper-based practices toward automated processes for data collection, analysis, reporting, and monitoring. Boubouh and Ghanim state that digitalization modernizes internal control systems through automated solutions that enable faster and more accurate data collection, analysis, and communication. They also emphasize that technologies such as artificial intelligence, advanced data analytics, and blockchain support anomaly detection, improve transaction security, and enhance the quality of information used in decision-making processes (Boubouh & Ghanim, 2025).

One important area of this transformation is the use of input controls in electronic accounting systems. These controls allow the system to check whether entered data complies with predefined rules regarding format, amount, date, account code, document number, and mandatory fields. Dhahir, Qassim, and Abbas underline the importance of automatic data validation, number-date-amount checks, prevention of duplicate entries, and completion of mandatory fields in detecting and correcting errors in electronic accounting data processing environments (Dhahir, Qassim, & Abbas, 2025). Such controls reduce the likelihood that inaccurate, incomplete, or duplicate financial data will enter the system and thereby strengthen the reliability of subsequent reporting processes.

Automated controls are also widely used in workflow and approval processes. In ERP environments, transactions such as purchase requests, payment orders, invoice recording, inventory withdrawals, and payroll processing can be routed automatically according to predefined authorization levels. This structure helps ensure that transactions are processed by authorized personnel and remain within approved limits. Shakkur notes that the automation of routine processes, including data entry, approvals, and reconciliations, reduces

the risk of error and enables organizational resources to be directed toward more complex tasks (Shakkur, 2023).

Access controls constitute another essential component of automated internal control in digital organizations. Through usernames, passwords, multi-factor authentication, role-based authorization, transaction limits, and system logs, organizations can define which users may access specific modules, datasets, and transaction functions. In ERP systems, these controls support segregation of duties by combining access restrictions with approval workflows, thereby reducing the risk of unauthorized activity, error, or fraud (Shakkur, 2023).

Exception and anomaly controls further enhance the effectiveness of digital internal control systems, particularly in organizations with high transaction volumes. These controls can automatically identify unusual transaction amounts, records created outside normal working hours, payments exceeding predetermined thresholds, repeated payments to the same bank account, or violations of authorization rules. In the General Motors example, Shakkur explains that ERP systems can flag transactions that exceed a specified threshold or breach a defined rule for internal control review (Shakkur, 2023). This type of automated detection allows organizations to identify control deviations more rapidly than would be possible through purely manual review.

Audit trail controls also play a central role in digital control environments. In digital systems, log records make it possible to trace who performed a transaction, when it was performed, under which authority, based on which prior data, and with what type of modification. These records are critical for investigating control deficiencies, evaluating fraud indicators, and demonstrating compliance with legal or regulatory requirements. ERP systems support this function by providing audit trails for transactions and system activities, thereby contributing to the monitoring of data changes, the identification of potential control issues, and the documentation of regulatory compliance (Shakkur, 2023).

However, the mere presence of automated controls does not guarantee internal control effectiveness. Automated controls can function

properly only when system rules are appropriately designed, authorization matrices are kept current, user access rights are reviewed periodically, system changes are managed under controlled procedures, and automated alerts are actively followed up. Otherwise, automated controls may become formal mechanisms that appear to exist in the system but fail to reduce the relevant risks in practice. For this reason, automated controls should be evaluated in connection with COSO's risk assessment, control activities, information and communication, and monitoring components.

4.3. Preventive and Detective Controls

In internal control systems, controls can generally be classified as preventive, detective, and in some cases, corrective/compensatory controls. This distinction is even more important in digital organizations because systems can prevent errors before a transaction occurs, detect errors after the transaction, or reduce control weaknesses through compensatory mechanisms.

Preventive controls aim to prevent risk before errors, fraud, unauthorized transactions, or violations of regulations occur. For example, checking user authorization before a transaction, limiting payment limits by the system, preventing registration without filling in mandatory fields, preventing duplicate invoice entries, enforcing separation of duties rules by the system, and preventing payments without approval are examples of preventive controls. In the study by Dhahir, Qassim, and Abbas, automatic data validation, date-amount verification, preventing duplicate data entry, and filling in mandatory fields are listed among the basic control methods used in electronic environments (Dhahir et al., 2025).

The power of preventive controls in digital systems stems from the fact that the control is embedded in the transaction flow. In manual environments, it is possible for employees to skip, forget, or incorrectly apply control procedures. In contrast, system-based preventive controls can prevent a process from proceeding unless it meets certain conditions. For example, the system may prohibit an unauthorized

user from changing a supplier's bank account; payments exceeding a certain amount may not be processed without second approval; or the creation of a second entry with the same invoice number may be prevented. In this respect, preventive controls reduce the likelihood of errors and fraud in digital organizations.

Detective controls, on the other hand, are controls aimed at identifying errors or nonconformities after they occur. Reconciliations, exception reports, log reviews, unusual transaction analyses, budget-actual comparisons, audit trail analyses, daily compliance reports, and system alerts are among the detective controls. Dhahir, Qassim, and Abbas describe real-time process monitoring, discrepancy and deviation detection, exception reports, daily compliance reports, error reports, and trend/deviation analyses as important components of internal control systems in the context of electronic financial statements (Dhahir et al., 2025).

Detective controls become particularly important when preventive controls are bypassed, poorly designed, or insufficient. For example, a user may have acted within their authorization limits, but the transaction amount, transaction time, or counterparty relationship may be unusual. In this case, the system needs to generate real-time alerts or signal the auditor with periodic exception reports. Boubouh and Ghanim state that artificial intelligence and machine learning technologies can analyze large amounts of data in real time to detect anomalies or suspicious behavior, thereby strengthening fraud prevention and detection processes (Boubouh & Ghanim, 2025).

Corrective controls, on the other hand, aim to remedy the detected error or control deficiency. Identifying the source of the error, recording the correction, informing responsible parties, updating the system rule, and designing additional controls to prevent recurrence are all within the scope of corrective controls. Dhahir, Qassim, and Abbas describe corrective actions in the electronic financial data environment as identifying the source of the error and documenting the corrective actions (Dhahir et al., 2025).

In digital organizations, the strongest internal control structure is one where preventive and detective controls work together. Relying solely

on preventive controls is insufficient because system rules may be poorly defined, authorizations may be incorrectly granted, or new risks may arise. Similarly, relying solely on detective controls is inadequate because even if errors or fraud are detected after they have occurred, financial, operational, or reputational damage may have already taken place. Therefore, the ideal approach in digital internal control systems is a combination of automated blocking before the transaction, real-time monitoring during the transaction, and exception analysis after the transaction.

4.4. Separation of Duties in ERP Systems

Separation of duties is one of the most fundamental principles of internal control systems. This principle aims to prevent the same person from performing critical stages such as initiating, approving, recording, protecting assets, and reconciling a transaction. The main goal is to reduce the possibility of a single person making a mistake or committing fraud and concealing it. In ERP systems, separation of duties becomes more complex than a manual organizational structure because it is no longer just about job descriptions, but also about system roles, user permissions, module access, approval flows, and transaction limits.

ERP systems bring together different business functions on a single database and integrated system. This structure increases data integrity in processes such as finance, accounting, purchasing, inventory, human resources, and production. However, it can also increase the risk of separation of duties if incorrect authorization is given. According to Shakkur, ERP systems increase operational efficiency, provide data visibility, and strengthen financial management processes by integrating business functions into a single system (Shakkur, 2023). However, this integrated structure requires strong access control and separation of duties design. In ERP systems, separation of duties controls are generally established through role-based access management. Each user should only be assigned the permissions they need to perform their task. For example, an employee creating a purchase request

should not have the authority to open a supplier card, approve payments, or change bank information. Similarly, a user who records invoices should not be able to create and approve payment orders alone, creating a weak control. Shakkur's study states that ERP systems support separation of duties by providing access controls and approval workflows, and reduce the risk of errors or fraud by preventing a single person from having excessive control over a particular process (Shakkur, 2023).

Segregation of duties in ERP systems can be strengthened through a structured authorization governance process that begins before access rights are assigned and continues throughout the system's use. This process should initially involve documenting business workflows, identifying sensitive or high-risk activities, determining combinations of duties that may create control conflicts, and developing a role-based authorization matrix. Once this structure is established, user access should be granted only within the boundaries of approved roles, while exceptional or temporary permissions should be time-limited and subject to appropriate review. Transactions with significant financial or operational implications should also be supported by layered approval mechanisms. The effectiveness of segregation of duties controls depends not only on initial design but also on continuous oversight. Therefore, access rights should be reviewed periodically, permissions of departing employees should be removed without delay, changes in job responsibilities should be reflected in the ERP system, and detected SoD conflicts should be reported and addressed in a timely manner.

In small businesses or organizations with limited personnel, it may not always be possible to fully ensure separation of duties. In this case, compensatory controls come into play. Adeboye, Ifeanyi, and Labisi state that in situations where separation of duties cannot be implemented due to personnel shortages, compensatory controls such as owner-level approvals, external accountant reviews, automated audit trails, and system alerts can be used (Adeboye, Ifeanyi, & Labisi, 2021). This approach is also valid for digital organizations. Especially in small and medium-sized enterprises, the lack of separation

of duties can be reduced with system-based approvals, real-time transaction alerts, and regular independent reviews.

A significant portion of separation of duties violations in ERP systems stem from managerial, not technical, reasons. Granting users excessive privileges to "speed things up," failing to revoke privileges from previous roles, allowing unlimited access for administrative users, or the uncontrolled use of emergency privileges all increase these risks. Therefore, separation of duties in an ERP environment is not solely the responsibility of the IT department; it is a shared responsibility of internal audit, accounting, finance, human resources, process owners, and senior management.

4.5. Control Deficiencies in Digital Systems

In digital systems, control deficiencies differ from traditional control deficiencies in that they have both process and technology dimensions. While control deficiencies in manual environments mostly manifest as lack of approval, insufficient documentation, lack of reconciliation, or breaches of division of labor; in digital systems, additional risks such as authorization matrix errors, system configuration deficiencies, weak password policies, lack of log record monitoring, data integrity issues, algorithmic errors, cybersecurity vulnerabilities, and poorly designed automated controls are observed.

Although digital technologies can significantly strengthen internal control systems, their use also introduces new layers of complexity. Boubouh and Ghanim argue that digital technologies contribute to internal control by reducing human error, accelerating control processes, and enabling real-time monitoring. However, they also create challenges related to data security, privacy, technological incident management, implementation costs, and organizational resistance to change (Boubouh & Ghanim, 2025). Therefore, the mere adoption of technology in a digital control environment should not be interpreted as evidence of a strong internal control system. The effectiveness of digital controls depends on how appropriately they are designed, configured, monitored, and integrated into the broader governance structure.

One of the most critical control weaknesses in digital systems concerns the management of access rights. Internal control risks increase when users are granted broader privileges than required for their responsibilities, when access rights of former employees are not revoked in a timely manner, when shared user accounts are used, when administrator privileges are not properly restricted, or when critical system changes are not monitored. Such deficiencies may create opportunities for unauthorized transactions, manipulation of data, or concealment of fraudulent activities. Although ERP systems can support access control, these mechanisms can produce effective results only when they are properly configured, periodically reviewed, and continuously monitored (Shakkur, 2023).

Another major source of weakness relates to the design of automated controls. The existence of an automated control does not necessarily mean that the related risk is adequately addressed. For instance, a payment threshold may be embedded in the system, but if transactions exceeding that threshold do not require an additional approval, the control may remain insufficient. Similarly, a duplicate invoice control that relies solely on invoice numbers may fail to detect irregularities if it does not also consider supplier information, invoice dates, and transaction amounts. Therefore, the logic of automated controls must be designed in line with the nature of the underlying risk. Mo emphasizes that digital transformation can make control activities more intelligent, yet this effect depends on a systematic control design that is consistent with the components of the COSO framework (Mo, 2023).

Monitoring activities also represent a key area of vulnerability in digital control environments. Digital systems produce large volumes of logs, alerts, exception reports, and user activity records. However, these records do not contribute to internal control effectiveness unless they are reviewed, analyzed, and linked to corrective action. Weaknesses may arise when system alerts are ignored, exception reports are not evaluated, user activities are not reviewed, or control deficiencies are not reported in a timely manner. Batte states that monitoring activities should assess not only whether controls exist but also whether they operate effectively, and identified deficiencies should be communicated without delay (Batte, 2025). In this respect,

monitoring in digital organizations should not be limited to the automatic generation of system records; it should also include the active interpretation of these records by responsible personnel and the initiation of appropriate remedial actions.

Data integrity and data quality problems constitute another important control risk. Since decision-making and reporting processes in digital systems largely depend on system-generated data, inaccurate, incomplete, duplicate, inconsistent, or manipulated data can weaken the reliability of internal controls. ERP systems may improve data consistency by creating a single source of information, but this benefit can be undermined by incorrect data entry, weak validation controls, poor master data management, or faulty system integrations. Shakkur notes that ERP systems support financial statement reliability through data accuracy, real-time monitoring, and audit trails (Shakkur, 2023). However, these advantages can be realized only when input controls, validation mechanisms, reconciliation procedures, and data governance practices operate effectively.

The integration of cybersecurity and privacy risks into the internal control system is also essential in digital organizations. Financial reporting data, customer records, supplier information, personnel files, and strategic business information are increasingly stored and processed through information systems. As a result, unauthorized access, data leakage, ransomware attacks, system interruptions, and other cyber incidents may directly threaten the core objectives of internal control. Boubouh and Ghanim indicate that while digital technologies enhance internal control capabilities, they also generate new risks such as cybersecurity threats and systemic vulnerabilities, which should be addressed through preventive and corrective control mechanisms (Boubouh & Ghanim, 2025). For this reason, cybersecurity and data privacy should not be treated as separate technical issues; they should be incorporated into the overall internal control framework.

Change management is another area in which digital systems may generate significant control weaknesses. Software updates, ERP module modifications, changes in control rules, new system integrations,

and data migration processes can all affect the reliability of existing controls. If a system change is transferred to the live environment without proper authorization, testing, documentation, and post-implementation review, an effective control may become disabled or a new vulnerability may be introduced. Therefore, change management controls should ensure that system modifications are approved, tested, documented, and monitored after implementation.

Overall, control deficiencies in digital systems do not arise solely from human error. They may also result from weaknesses in technology design, data architecture, authorization management, monitoring practices, cybersecurity governance, and change management processes. For this reason, internal control systems in digital organizations should address technological, procedural, human, and governance dimensions together, in line with the five components of the COSO framework. An effective digital internal control system should benefit from automated controls, while also ensuring that these controls are properly designed, regularly monitored, updated when necessary, and reported through a reliable governance mechanism.

Chapter Summary

This section addresses the transformation of internal control systems in digital organizations. It emphasizes that internal control is no longer limited to manual approvals, document checks, reconciliations, and traditional separation of duties practices; it has transformed into a technology-supported, data-driven, and continuously traceable governance mechanism.

The COSO framework is examined as a fundamental reference model for the design and evaluation of internal control systems in digital organizations. The section explains how the control environment, risk assessment, control activities, information and communication, and monitoring activities relate to ERP systems, automated workflows, artificial intelligence, blockchain, and real-time reporting tools.

Furthermore, automated controls, preventive and detective controls, and the separation of duties in ERP systems are discussed. It is noted that automated controls increase transaction reliability, reduce human error, support access management, and strengthen traceability through system logs and digital audit trails. However, it is stressed that the mere existence of automated controls is insufficient; these controls must be properly designed, regularly monitored, updated, and aligned with the organization's risks.

Finally, the chapter addresses key control deficiencies observed in digital systems. Weak access management, poorly designed automated controls, inadequate monitoring activities, data integrity issues, cybersecurity risks, and weak change management controls are identified as prominent control weaknesses in digital organizations. Overall, the chapter concludes that an effective internal control system in digital organizations is possible only through a combination of technology, process discipline, human accountability, and strong governance principles.

Chapter 5 – Cybersecurity and Information Systems Auditing

Introduction

Digitalization has made businesses largely dependent on information technology for financial reporting, accounting information systems, payment processes, supply chains, and management decision-making mechanisms. While this transformation provides businesses with advantages such as speed, automation, and data-driven decision-making, it has also brought significant cyber risks such as data breaches, unauthorized access, ransomware, phishing attacks, social engineering, and system disruptions.

Therefore, cybersecurity is no longer considered merely a technical IT issue; it is a strategic area directly related to corporate governance, internal control, risk management, and audit quality. The internal audit function evaluates whether cybersecurity controls are adequately designed and functioning effectively, providing independent assurance to the board of directors and the audit committee.

This section addresses cybersecurity fundamentals, access management risks, user authorization controls, data privacy and GDPR/KVKK compliance, phishing and social engineering risks, and incident response processes from the perspective of internal audit and information systems audit.

5.1. Fundamentals of Cybersecurity

Cybersecurity refers to the protection of data, networks, applications, devices, and information processing infrastructures in digital systems against the risks of unauthorized access, modification, destruction, interruption, or misuse. In the context of information systems, the main objective of cybersecurity is to protect the confidentiality, integrity, and availability of information. Confidentiality means that

information is accessible only by authorized persons; integrity means ensuring the accuracy and unaltered nature of the information; and availability means that systems and data are available when needed. Shafa and Islam state that in the context of accounting information systems, cybersecurity is the technical basis that protects the confidentiality, integrity, and availability of financial data; encryption, multi-factor authentication, intrusion detection systems, and audit logs are among the fundamental elements of this structure (Shafa and Islam, 2025, Alzeban et al., 2026).

Cybersecurity risks today are not only technical risks that information technology departments need to manage. Siyaya et al. emphasize that cybersecurity risk constitutes a business risk and that internal audit plays a significant role in addressing these risks in an integrated manner with management, risk management, and internal control processes (Siyaya et al., 2025). In this context, cybersecurity is a broad risk area that can have operational, financial, legal, and reputational consequences that may hinder a business from achieving its strategic goals (Calvin et al, 2025).

Cybersecurity fundamentals can be evaluated under three main control areas from an audit perspective: administrative controls, technical controls, and physical controls. Administrative controls include elements such as information security policies, procedures, job and responsibility definitions, risk management processes, awareness training, and management oversight. Technical controls consist of firewalls, intrusion detection and prevention systems, data backup, encryption, access control systems, multi-factor authentication, and security monitoring tools. Physical controls relate to the physical security of server rooms, data centers, backup areas, and critical equipment. Siyaya et al. Internal auditors should evaluate administrative, technical, and physical controls together in cybersecurity audits (Siyaya et al., 2025).

From an information systems audit perspective, the primary objective of cybersecurity is not only to verify the existence of existing controls but also to assess whether these controls are adequate, effective, and aligned with business risks. Therefore, the auditor should ask "which control is designed for which risk?" before asking "does a control

exist?". For example, a business may implement multi-factor authentication; however, if this application is only valid for senior managers and disabled or weakened by exceptions for critical financial system users, it is not possible to talk about the effectiveness of the control. The aim of the audit is to examine not only whether the control exists in the documents but also whether it actually works and whether it reduces risks to a reasonable level. Adesokan-Imran's work indicates that cybersecurity governance is a fundamental element in protecting critical infrastructure, and that the NIST Cybersecurity Framework and ISO/IEC 27001 and 27002 standards offer widely used structured frameworks for managing risks (Adesokan-Imran, 2025). The NIST framework is built on the functions "Identify, Protect, Detect, Respond, Recover." This structure is also useful from an audit perspective; because the auditor can separately assess whether the organization has identified its assets and risks, established protection controls, has the capacity to detect incidents, has response processes, and has recovery capabilities.

The fundamental assurance question in a cybersecurity audit can be formulated as follows: Has the organization identified cyber risks that could affect its critical information assets and business processes, designed appropriate controls to address these risks, monitored the functioning of controls, and established the capacity for response and recovery when an incident occurs? This question shows that a cybersecurity audit is not merely a firewall, antivirus, or encryption test; rather, it is a holistic activity linked to corporate risk management, governance, process ownership, and audit evidence production.

The basis of a cybersecurity audit is not merely verifying the existence of security controls, but systematically evaluating how these controls are linked to standards, frameworks, and business risks. The integrated cybersecurity audit framework developed by Al-Matari et al. emphasizes collaboration between information systems auditors and cybersecurity experts, structuring the audit process around four main control components: physical, administrative, data, and technical controls. This approach demonstrates that a cybersecurity audit is not limited to technical vulnerability scanning or penetration testing; it requires a comprehensive approach encompassing physical security, policies and

procedures, data leakage prevention, access control, log review, incident investigation, and technical testing (Al-Matari et al., 2021).

According to this framework, a cybersecurity audit can be conducted using a two-stage logic. In the first stage, physical, administrative, and data controls are examined to assess the organization's overall security posture, and potential control gaps are reported. In the second stage, technical controls are implemented; more in-depth tests such as information gathering, vulnerability assessment, penetration testing, and digital forensics are applied. Thus, the audit first evaluates the control environment and governance structure, and then proceeds to generate technical evidence where necessary. This structure is important for internal auditing because the auditor is not obliged to use all technical tools directly, but must understand which technical test is necessary in which control area and how the findings relate to business risk (Al-Matari et al., 2021).

5.2. Access Management Risks

Access management is the process of determining, implementing, monitoring, and, if necessary, revoking access to information systems by whom, with what permissions, for how long, and under what conditions. This area is one of the most critical issues in cybersecurity and information systems auditing because many cyber incidents stem from access management vulnerabilities such as weak password practices, over-authorization, failure to close accounts of departing personnel, shared user accounts, failure to monitor privileged accounts, or failure to implement multi-factor authentication.

Access management represents a critical control area in accounting information systems, particularly because weaknesses in authorization structures may directly affect the reliability, confidentiality, and integrity of financial information. One of the most important risks in this context is unauthorized access, which occurs when users are able to view, modify, or process system functions and data beyond the scope of their job responsibilities or business needs. In accounting information systems, such access may result in the alteration of financial

records, manipulation of payment instructions, disclosure of customer or employee information, or deletion of audit trails. Shafa and Islam emphasize that role-based access controls in accounting information systems restrict users to the data and functions relevant to their duties, thereby reducing the likelihood of internal misuse (Shafa & Islam, 2025).

A related access management weakness arises when users are granted broader privileges than required for their assigned tasks. Excessive authorization creates significant control vulnerabilities, especially in ERP and accounting information systems where multiple financial processes are integrated. For instance, allowing the same user to create suppliers, initiate payment orders, and approve bank payment files would undermine the principle of segregation of duties. Such authorization combinations may increase the risk of fictitious supplier creation, fraudulent invoice processing, and unauthorized payments. Therefore, access management audits should not be limited to reviewing user lists; they should also examine combinations of permissions across key business processes and assess whether these combinations create incompatible duties (Andreanov & Maisyarah, 2025).

Privileged user accounts constitute another high-risk area within access management. System administrators, database administrators, security administrators, and application administrators typically have extensive authority over critical systems and data. If these privileges are misused or inadequately monitored, the consequences may include unauthorized modification of system records, deactivation of security controls, or extraction of sensitive data. For this reason, privileged accounts should be subject to stronger control procedures, including robust authentication, session logging, periodic access reviews, segregation of duties, and additional approval mechanisms for critical system operations.

Access risks may also emerge when user lifecycle management is not properly maintained. Changes such as recruitment, promotion, transfer to another department, modification of job responsibilities, or termination of employment require timely updates to user access rights. If these changes are not reflected in the system, employees may retain permissions that are no longer necessary for their duties. This risk

becomes particularly significant when the accounts of former employees remain active after departure. In access management audits, human resources records should therefore be reconciled with system user lists, and particular attention should be given to former employee accounts, inactive users, and accounts that have not been used for extended periods.

Weak authentication practices further increase exposure to unauthorized access. Inadequate password policies, absence of multi-factor authentication, and the use of shared accounts make systems more vulnerable to both internal misuse and external attacks. Aeni and Mais show that external auditors use measures such as data encryption, multi-factor authentication, role-based access controls, and system resilience testing to protect client data (Aeni & Mais, 2026). This indicates that access security is not only a technical control issue but also a factor that directly affects audit quality, data protection, and the reliability of audit processes.

The audit of access management risks should ultimately focus on whether the organization applies the principle of least privilege in practice. Under this principle, users should be granted only those access rights that are necessary to perform their assigned responsibilities. The effectiveness of this principle can be assessed through user access matrices, job descriptions, authorization request forms, system logs, privileged account listings, and periodic access review records. By examining both individual permissions and permission combinations, auditors can evaluate whether access rights are appropriately restricted, monitored, and aligned with the organization's internal control objectives.

The auditor should also establish the connection between access management and business processes. For example, the auditor should examine which systems are used in purchasing, payment, payroll, inventory, financial reporting, and customer data management processes, who accesses these systems, who can perform critical operations, and whether these operations are subject to approval mechanisms. Thus, access management auditing moves beyond being merely a technical user account control; it transforms into an internal

control assessment linked to risks of financial error, fraud, data breaches, and operational disruptions.

5.3. User Authorization Controls

User authorization audits are systematic audit activities that evaluate whether user access rights are properly defined in information systems, whether authorizations are consistent with job descriptions and business needs, whether authorization changes are made in a timely manner, and whether critical operations are subject to appropriate approval mechanisms.

A user authorization audit should begin with an assessment of the organization's access management framework. The auditor is expected to determine whether the organization has formalized policies and procedures governing the creation, modification, monitoring, and termination of user access rights. Such policies should address the full access lifecycle, including user account creation, authorization approval, role changes, access revocation, password requirements, multi-factor authentication, privileged account management, remote access, third-party access, and periodic access reviews. In cybersecurity audits, the review of administrative security controls is particularly important, as policies and procedures designed to protect critical infrastructure form a key component of the control environment (Siyaya et al., 2025).

A central part of this audit process is the evaluation of the authorization matrix. The authorization matrix provides a structured view of user roles, system functions, and the level of access granted to each role. The auditor should examine whether this matrix is current, aligned with job descriptions, and designed in a way that supports the segregation of critical duties. This assessment is especially important in ERP environments, where purchasing, payment, inventory, accounting, banking, and reporting modules are often interconnected. The auditor should therefore evaluate whether any user has excessive or conflicting permissions, particularly where the same individual can initiate, approve, record, and report the same transaction.

The audit should also include detailed testing of user access rights. By selecting users from the active user list, the auditor can compare each user's current job description with the permissions assigned in the system. Access rights that are inconsistent with the employee's role should be treated as potential authorization weaknesses. For instance, if an employee working in the sales department has permission to modify supplier bank account details, this would indicate a significant control deficiency because the access granted is not compatible with the employee's operational responsibilities.

Another critical area is the timely removal or adjustment of access rights when employees leave the organization or change positions. The auditor should compare human resources records with system user records to determine whether the accounts of former employees were disabled within an appropriate timeframe. Similarly, when employees are transferred to different roles, their previous permissions should be reviewed and revoked where they are no longer necessary. This control is essential for reducing the risk of unauthorized access and insider misuse.

Privileged user accounts require separate audit attention due to the broad authority assigned to such users. System administrators, database administrators, application administrators, and security administrators may have access rights that allow them to modify system configurations, create users, change permissions, or access sensitive data. The auditor should identify privileged users, examine the approval basis for their access rights, assess whether their activities are adequately logged, and determine whether these logs are reviewed by an independent party. Without independent monitoring, privileged access may create a serious control risk.

Periodic access review is another key component of user authorization control. Organizations should regularly reassess user permissions and remove access rights that are no longer required for business purposes. These reviews should not be limited to a formal signature process over user lists. Instead, process owners should compare actual job responsibilities with system permissions and confirm whether each access right remains justified. The auditor should therefore

review access recertification records, assess whether the review was performed substantively, and determine whether identified exceptions were followed by corrective action.

The effectiveness of a user authorization audit also depends on the quality and sufficiency of audit evidence. Relevant evidence may include active user lists, authorization matrices, access approval records, system logs, human resources records, job descriptions, access change requests, password policies, privileged account reports, and periodic access review documentation. Cybersecurity and information security audits are generally supported by predefined checklists, control assessments, corrective action tracking, and systematic documentation of audit data for reporting purposes. Antunes et al. (2022) emphasize that these processes can be time-consuming and that audit data should be stored in a structured manner to support reporting, follow-up, and control evaluation.

In this context, the output of user authorization audits should not be simply "permissions are appropriate/inappropriate." The auditor should clearly state what business risk the authorization vulnerability creates. For example, a finding such as "User X having simultaneous permissions to modify supplier bank accounts and create payment files increases the risk of unauthorized payments and fraudulent supplier transactions" is more valuable from a management perspective because it links the technical observation to the company risk. The tools used in cybersecurity audits are an important supporting element in terms of their capacity to produce audit evidence. In the study by Al-Matari et al., cybersecurity audit tools are classified under four main tasks: information gathering, vulnerability assessment, penetration testing, and digital forensics investigation. Information gathering tools provide data on domain names, IP structures, system information, employee emails, organizational profiles, and technical infrastructure. Vulnerability assessment tools aim to identify open ports, misconfigurations, unpatched services, application vulnerabilities, and operating system vulnerabilities. Penetration testing tools test the exploitability level of systems from an attacker's perspective. Forensic computing tools are used to examine log files, disk images, deleted data, and digital evidence (Al-Matari et al., 2018).

The use of these tools does not mean that the auditor replaces the technical expert. On the contrary, the information systems auditor should interpret the test results obtained from the technical teams within the context of internal control, risk management, and corporate governance. For example, detecting an open port in a vulnerability scan is a technical finding; however, the main assessment from an audit perspective is which critical business process, which data asset, which financial or operational risk is affected by this open port, and whether management accepts this risk. Therefore, cybersecurity tools should be seen as technical support tools that facilitate evidence production in the audit process; the final audit judgment should be formed by evaluating risk, control design, control operation, and business impact together. Using audit tools adaptable to customer or organizational characteristics in information systems audits provides a significant advantage, especially for SMEs. Antunes et al. note that SMEs often lack the complex audit tools, high technological maturity, or established information security teams designed for large businesses. Therefore, the developed web-based audit system allows checklists from different standards to be uploaded to the system, actions and corrective measures to be defined for each control, and the audit process to be monitored in a central database (Antunes et al., 2022).

This finding points to an important aspect of internal auditing: Cybersecurity audits should not be implemented with the same scope and depth in every business. While large-scale, technologically mature organizations may utilize detailed penetration testing, advanced log correlation systems, and continuous monitoring tools, small or medium-sized enterprises may prioritize basic access controls, backup, policy documentation, awareness training, data classification, and the protection of critical systems. Therefore, the audit approach should be based on standards but adapted to the size, sector, technological maturity, and risk profile of the organization.

5.4. Data Privacy and Compliance with the General Data Protection Regulation (GDPR) / Personal Data Protection Law (KVKK)

Data privacy refers to the lawful, ethical, secure, and purpose-bound processing of personal data. In digital businesses, data privacy is not solely the responsibility of the legal department or compliance department; it is directly related to information systems, internal control, financial reporting, auditing, and corporate governance. This is because unlawful processing of personal data, data breaches, unauthorized access, or data leaks not only lead to administrative fines but also negatively impact customer trust, investor perception, financial transparency, and corporate reputation. Shafa and Islam define data privacy as the lawful and ethical management of personal and sensitive information; they consider consent, purpose limitation, data minimization, and retention period control as fundamental principles of privacy governance (Shafa and Islam, 2025). In the context of accounting information systems, these principles require the protection of sensitive data such as employee payroll records, customer transactions, supplier invoices, bank information, and management reports against unauthorized access.

The auditor's primary task in terms of GDPR and KVKK compliance is to evaluate the organization's personal data processing processes not only in terms of formal compliance with the legislation, but also in terms of information systems controls. While GDPR is a comprehensive regulation on the protection of personal data in the context of the European Union, KVKK constitutes the basic legal framework for the processing and protection of personal data in Turkey. The uploaded resources explicitly refer to GDPR; KVKK can be evaluated within the same data protection logic in the Turkish context. However, it should be noted that the specific articles and provisions of KVKK are not detailed in the uploaded resources; therefore, they are addressed not as a detailed legal interpretation, but within the framework of data protection principles similar to GDPR.

Vuko et al. state that GDPR is a significant coercive corporate pressure element within cybersecurity and privacy regulations, causing

organizations to integrate privacy protections into processes, services, and products (Vuko et al., 2025). However, the same study also notes that compliance alone is not sufficient for cybersecurity audit effectiveness; internal auditor competence, board support, and cooperation with the first/second line of defense are also shown to be critical (Vuko et al., 2025).

A data privacy audit should begin with a clear understanding of the organization's data inventory. The organization is expected to identify what types of personal data it collects, the purposes for which such data are processed, where the data are stored, with whom they are shared, how long they are retained, and which security controls are used to protect them. Without a reliable and up-to-date data inventory, it is difficult to conclude that data privacy compliance is being managed effectively. The data inventory therefore provides the foundation for evaluating whether personal data processing activities are lawful, controlled, traceable, and aligned with organizational responsibilities.

Purpose limitation and data minimization are also central to data privacy compliance. Organizations should collect and process only the personal data that are necessary for legitimate business purposes. The collection of excessive or irrelevant data may create legal, operational, and ethical risks. For example, requesting special categories of personal data that are not necessary for service delivery during customer registration may indicate a weakness in data minimization practices. From an audit perspective, this assessment requires the review of system forms, customer registration screens, human resources data entry fields, ERP datasets, and other digital interfaces through which personal data are collected or processed.

Access and authorization controls constitute another critical element of a data privacy audit. Access to personal data should be granted on a task-based and need-to-know basis, and only authorized users should be able to view, modify, export, or delete such data. Role-based access control helps reduce the risk of internal misuse by ensuring that users can access only the information required for their duties. Shafa and Islam (2025) emphasize that role-based access mechanisms can reduce internal

misconduct risks by limiting users' ability to view or modify data beyond the scope of their responsibilities.

Retention and destruction processes should also be evaluated as part of the audit. Personal data should not be retained indefinitely once the original processing purpose has expired. Organizations should define retention periods and implement deletion, destruction, or anonymization procedures at the end of those periods. The auditor should therefore review the organization's retention and destruction policies, system-based deletion records, archiving practices, and evidence showing whether obsolete personal data are removed or anonymized in accordance with the relevant rules.

The data breach response process is another essential area of review. A meaningful data privacy audit should assess how the organization detects, classifies, reports, investigates, and remediates data breaches. It should also examine whether notifications are made within the required timeframe and whether corrective actions are monitored until completion. Loumachi et al. (2026) show that incident response, evidence integrity, record keeping, traceability, and reporting obligations are recurring operational requirements across regulatory and standard-setting frameworks such as GDPR/UK GDPR, NIS2, DORA, PCI DSS, ISO/IEC 27001, and NIST SP 800-53.

Third-party and cloud service provider risks should be considered within the same audit scope. Financial systems, cloud-based accounting platforms, payroll applications, customer relationship management systems, and outsourced data processing services may result in personal data being transferred outside the organization or processed by external parties. These arrangements create risks related to data ownership, confidentiality, access control, cross-border transfer, service provider dependency, and monitoring responsibilities. Shafa and Islam (2025) state that cloud-based accounting platforms and shared service centers require continuous monitoring and third-party risk management in order to protect data integrity across the supply chain.

From an internal audit perspective, GDPR/KVKK compliance should not be reduced to a formal review of legal documentation. Information notices, explicit consent forms, privacy policies, and

contractual clauses are important, but they do not by themselves provide sufficient assurance. The critical issue is whether data processing activities are supported by effective system-based controls. For instance, an organization may have a written personal data protection policy; however, if all accounting employees can access payroll data without role-based restrictions, the policy does not operate effectively in practice. Therefore, the auditor should evaluate data privacy compliance together with information systems controls, access management, logging, retention mechanisms, third-party governance, and breach response procedures.

5.5. Phishing and Social Engineering Risks

Phishing and social engineering are among the most important threat areas targeting human behavior within cybersecurity risks. Phishing attacks generally aim to obtain passwords, credentials, payment information, or sensitive data by deceiving users through fake emails, messages, links, or websites. Social engineering, on the other hand, is a broader concept; it is when an attacker uses human psychology, trust relationships, and behavioral weaknesses such as haste, obedience to authority, curiosity, or fear, rather than technical vulnerabilities, to lead individuals to make erroneous transactions.

Adesokan-Imran states that phishing attacks, exploitation of publicly available applications, and brute-force attacks stand out among current cyber threats to critical infrastructure (Adesokan-Imran, 2025). This finding shows that cybersecurity audits should focus not only on technical system vulnerabilities but also on user behavior and awareness levels.

Phishing risks are particularly critical for financial systems and accounting information systems. An attacker may send a fake administrator email requesting the creation of a payment instruction; A phishing attacker might redirect payments with a fake message stating that a supplier bank account has changed; request payroll data from a human resources employee; or trick accounting personnel into clicking a fake invoice link. Therefore, phishing should be considered not only

an information security problem but also a financial fraud, asset loss, and reporting reliability issue. Social engineering risks are strongly associated with the human dimension of cybersecurity. Although organizations may invest in technical security tools, weak user awareness can still expose business processes to phishing, impersonation, fraudulent payment instructions, and unauthorized data disclosure. In this respect, cybersecurity risk management requires not only technological safeguards but also sufficient competence among employees, IT professionals, and internal auditors. Siyaya et al. (2025) emphasize that cybersecurity risk management requires a new set of competencies for both IT professionals and internal auditors, while many employees still lack adequate technical knowledge in this area. This suggests that awareness training against phishing and social engineering attacks should be treated as an integral component of the internal control system rather than as a separate or optional training activity.

Weak verification and approval procedures also increase exposure to social engineering attacks. When critical transactions such as payment instructions, supplier bank account changes, or confidential data sharing are executed on the basis of a single email, the organization becomes vulnerable to manipulation. For this reason, sensitive requests should be supported by multi-channel verification, second-level approval, segregation of duties, and automated alerts for unusual transactions. For example, a supplier bank account change should not be approved solely through an email request; it should also be verified through a registered telephone number, an official supplier portal, or another independently validated communication channel.

Technical filtering controls have an important role in reducing phishing risk, but they cannot eliminate social engineering threats on their own. Email security gateways, malicious link scanning, domain validation, attachment scanning, endpoint protection, and device-level security controls may reduce the likelihood that harmful content reaches users. However, social engineering attacks often succeed by exploiting trust, urgency, authority, fear, or routine behavior. Therefore, technical filters should be supported by continuous awareness training, behavioral testing, and practical simulations that evaluate how users respond to suspicious requests in real business contexts.

The misuse of senior management identity is another significant social engineering risk. In CEO fraud and business email compromise schemes, attackers may impersonate senior executives and request urgent payments, confidential transactions, or sensitive data transfers. Such attacks are particularly dangerous because employees may feel pressured to bypass ordinary procedures when the request appears to come from a person in authority. The auditor should therefore examine whether the organization has defined clear verification and approval procedures for unusual, urgent, or high-risk requests, regardless of the apparent sender's hierarchical position.

From an internal audit perspective, phishing and social engineering audits should include both documentary and behavioral evidence. Relevant procedures may include reviewing cybersecurity awareness training records, evaluating phishing simulation results, analyzing previous incident records, assessing email security controls, testing second-approval mechanisms in payment processes, reviewing supplier information change procedures, and examining whether users are aware of suspicious incident reporting channels. These procedures allow the auditor to evaluate not only whether formal controls exist, but also whether employees understand and apply them in practice.

The organization's incident reporting culture is also a critical element of social engineering resilience. If employees hesitate to report suspicious emails, accidental clicks, or possible credential exposure, incidents may remain undetected until they cause greater damage. For this reason, organizations should promote a cybersecurity culture based on learning, early reporting, and timely escalation rather than punishment. Shafa and Islam (2025) argue that security culture, employee awareness, ethical leadership, and compliance orientation influence the effectiveness of technical controls. This perspective indicates that social engineering risk cannot be addressed solely through technical safeguards; it must also be managed through organizational behavior and culture.

The main contribution of social engineering auditing is that it places the human factor at the center of the control environment. Even if an organization has encryption, firewalls, intrusion detection systems,

and access controls, its cybersecurity posture may remain weak if employees are vulnerable to fraudulent payment requests, fake login pages, impersonation attempts, or deceptive data-sharing instructions. Therefore, internal audit should assess social engineering risks not only by checking whether information security training has been delivered, but also by evaluating how behavioral controls operate within actual business processes.

Social engineering risks are also linked to social and behavioral testing controls within integrated cybersecurity audit frameworks. Al-Matari et al. (2021) associate such controls with the first line of defense, where social testing is used to assess employee behavior in relation to organizational assets, security awareness, and vulnerability to aggressive manipulation. This approach broadens the scope of cybersecurity auditing by recognizing that employees' responses to manipulation attempts are themselves part of the control environment.

Accordingly, phishing and social engineering audits should not be limited to reviewing training attendance records or policy documents. The auditor should assess the organization's actual behavioral resilience against social engineering attacks through controlled phishing simulations, fraudulent payment instruction scenarios, supplier bank account change tests, and suspicious email reporting exercises. The purpose of these procedures is not to punish employees, but to identify and reduce control weaknesses arising from human behavior. A stronger defense against social engineering risks can be established when management oversight, awareness training, social testing, incident reporting culture, and technical filtering controls operate together.

5.6. Incident Response Assessment

Incident response is the process of detecting, analyzing, containing, eliminating, and recovering systems after a cybersecurity incident, and reflecting the lessons learned in organizational controls. In organizations without an effective incident response structure, a small security incident can quickly turn into a data breach, system outage, financial loss, or

reputational crisis. Therefore, incident response assessment is an indispensable part of cybersecurity and information systems auditing.

Adesokan-Imran states that risk management is a fundamental element of cybersecurity governance and should be considered as a cyclical process consisting of risk assessment, risk analysis, and strategic mitigation phases. In this context, advanced security controls, monitoring mechanisms, and incident response protocols play an important role in reducing cybersecurity risks (Adesokan-Imran, 2025).

An incident response assessment should begin with an evaluation of whether the organization has a formal and comprehensive incident response plan. Such a plan should clearly define how cyber incidents are identified, classified, escalated, communicated, contained, investigated, and remediated. It should also specify responsibilities, evidence preservation requirements, legal notification obligations, recovery procedures, and internal communication channels. An effective incident response plan should not be limited to the IT department as a purely technical document. Instead, it should be integrated with the responsibilities of legal affairs, corporate communications, internal audit, risk management, senior management, human resources, and relevant business units.

A critical component of incident response capability is the organization's ability to detect incidents in a timely manner. This requires an appropriate combination of log management, intrusion detection systems, security monitoring tools, anomaly detection mechanisms, endpoint protection, and security operations processes. Without effective detection capacity, cyber incidents may remain unnoticed until they cause financial, operational, or reputational damage. Loumachi et al. (2026) identify continuous monitoring and anomaly detection as fundamental operational processes in cybersecurity compliance and auditing.

The classification and prioritization of incidents should also be assessed. Not every security alert has the same level of urgency or organizational impact. The auditor should evaluate whether the organization classifies incidents according to their likelihood, severity, business impact, and effect on critical systems. For instance, repeated failed login attempts may represent a low-level alert, whereas an

unusual data extraction by a privileged user should be treated as a high-criticality event. A mature incident response process should therefore distinguish routine security alerts from events requiring immediate escalation and management attention.

Response and containment capacity is another central area of audit evaluation. Once an incident is detected, the organization should be able to isolate affected systems, stop malicious activity, suspend compromised user accounts, prevent malware propagation, and protect unaffected systems. However, containment procedures must be carefully controlled because inappropriate intervention may destroy evidence, interrupt business continuity, or expand the impact of the incident. For this reason, the response process should combine technical procedures with clearly defined managerial approval and escalation mechanisms.

Evidence management and audit trail integrity are particularly important in cyber incident response. After an incident, log records, system images, access logs, email headers, network traffic records, endpoint activity records, and user activity data should be preserved in a reliable and traceable manner. The integrity of such evidence is essential for investigation, regulatory reporting, disciplinary action, legal proceedings, and subsequent internal audit review. Loumachi et al. (2026) emphasize that evidence integrity, traceability, record keeping, and audit trails are fundamental conditions for authority and assurance in cybersecurity compliance and auditing, including AI-enabled systems.

Incident response should also be evaluated in relation to recovery and business continuity. Following a cyber incident, affected systems must be restored securely, backups must be recovered, data integrity must be verified, and business processes must return to normal operations within an acceptable timeframe. Backup policies, disaster recovery plans, recovery time objectives, and recovery point objectives are therefore closely linked to incident response assessment. Siyaya et al. (2025) note that data backups constitute an important technical security control area that should be evaluated by internal audit.

An effective incident response process does not end when the immediate incident is closed. The organization should conduct a post-incident review to identify the root causes of the event, determine failed or insufficient controls, update relevant policies and procedures, revise employee training where necessary, and monitor corrective actions until completion. This learning process is essential for preventing similar incidents from recurring. Adesokan-Imran (2025) argues that the continuous evolution of cyber threats requires governance models to incorporate continuous threat monitoring, proactive risk mitigation, and strategic response capabilities.

From an audit perspective, incident response assessment should therefore examine both preparedness and actual operational effectiveness. The auditor should determine whether the organization has a written and tested incident response plan, whether roles and responsibilities are clearly assigned, whether critical incidents are detected and escalated in a timely manner, whether response steps are documented, whether evidence is preserved, whether legal and regulatory reporting procedures are defined, and whether post-incident root cause analysis is performed. The auditor should also assess whether corrective actions are monitored and whether the board of directors and audit committee receive sufficient information on significant cyber incidents.

Incident response auditing should not be limited to reviewing what happened after a cyber event. It should also assess whether the organization has a governance structure capable of detecting, managing, investigating, and learning from incidents. In the integrated cybersecurity audit framework proposed by Al-Matari et al. (2021), incident and risk management, business impact analysis, vulnerability assessment, digital forensics, formal risk acceptance, cybersecurity compliance, and internal control testing are positioned within the three lines of defense. In this structure, the first line monitors daily control processes through management reviews and technical or social testing; the second line evaluates emerging risks, business impacts, and vulnerabilities; and the third line, represented by internal audit, provides independent assurance through digital forensics, compliance assessment, and internal control testing.

Accordingly, incident response assessment should be understood as a broad assurance activity that connects cybersecurity operations with governance, risk management, legal compliance, business continuity, and internal control. The auditor's role is not merely to confirm the existence of an incident response plan, but to evaluate whether the organization can detect incidents early, respond effectively, preserve evidence, recover securely, report appropriately, and improve its control environment through post-incident learning.

This model clarifies the role of internal audit in incident response assessment. Internal audit should not directly undertake the technical resolution of the incident; instead, it should assess the existence of an incident response plan, the clarity of roles, the integrity of incident records, the preservation of evidence, the response time, the impact on business continuity, legal notification processes, and the monitoring of post-incident corrective actions. Digital forensics, in particular, is a critical control area for determining the source of the incident, its scope, and the integrity of evidence. Log files, disk images, recovered data, and system event logs should be used as essential audit evidence in the post-incident assurance process.

Chapter Summary

This chapter discusses the importance of cybersecurity and information systems auditing in digitized businesses. The fact that financial data, customer information, operational processes, and decision-making mechanisms are largely conducted through digital systems has made cybersecurity controls a fundamental element of the internal control system.

The chapter evaluates access management, user authorization, data privacy, phishing, social engineering, and incident response processes from an internal audit perspective. It emphasizes that these areas are not independent of each other; weak access management can lead to data breaches, insufficient user awareness to phishing attacks, and inadequate incident response plans to corporate crises.

Furthermore, it is stated that for cybersecurity auditing to be effective, the internal audit function must possess technical knowledge, a risk-based perspective, and sufficient audit competence. It is emphasized that the board of directors and the audit committee should treat cybersecurity as a strategic business risk, while internal audit should maintain its independent assurance role by working collaboratively with the first and second lines of defense.

In conclusion, this chapter demonstrates that cybersecurity and information systems auditing is not merely technical area of expertise; rather, it is a strategic audit area in terms of corporate governance, internal control, risk management, data privacy, business continuity, and digital assurance capabilities.

Chapter 6 – Data Analytics and Artificial Intelligence in Internal Audit

Introduction

Digitalization has significantly altered the working methods of the internal audit function. While the traditional audit approach was largely based on sample selection, manual document review, and periodic checks, today's internal audit is increasingly supported by data analytics, big data, artificial intelligence, and continuous process testing. This transformation enables auditors to analyze larger datasets, detect risky transactions earlier, and evaluate indicators of fraud more systematically.

This chapter covers fundamental concepts of audit analytics, the use of big data in internal audit, artificial intelligence applications, continuous process testing, fraud detection using analytical methods, and ethical risks associated with the use of artificial intelligence. The aim of this chapter is to explain how data analytics and artificial intelligence are transforming internal audit practices, the opportunities they present, and the risks that must be considered alongside them.

6.1. Fundamentals of Audit Analytics

Digitalization is fundamentally transforming the scope, working methods, and assurance generation of the internal audit function. For many years, the traditional internal audit approach relied on sample-based testing, manual document reviews, periodic control assessments, and historical findings. This approach has been somewhat sufficient for businesses with lower transaction volumes and more limited data sources. However, today's businesses generate large volumes of data from financial transactions, operational processes, customer movements, user access, supplier relationships, and digital platform activities. Therefore, internal audit relying solely on manual review and

limited sampling may be insufficient for detecting complex risks and hidden fraud patterns. According to Ilori et al. (2024), in the face of increasing complexity and technological advancements, traditional internal audit methods are inadequate for comprehensive risk assessment and effective fraud detection; advanced data analytics, on the other hand, offers a transformative approach that enhances the effectiveness of internal audit.

Audit analytics is the systematic process of collecting, cleaning, analyzing, and transforming financial, operational , information systems, compliance, and external environmental data into audit decisions within internal audit activities. This process is not limited to simply verifying the accuracy of past transactions. It also encompasses predicting future risks, early detection of control weaknesses, identification of fraud indicators, and directing audit resources to high-risk areas. In this respect, audit analytics transforms internal audit from a purely retrospective control activity into a proactive assurance mechanism that can foresee risks and provide timely warnings to management.

Audit analytics consists of different levels of analysis. Descriptive analytics reveals what is happening within the organization. For example, the number of payments made in a specific period, transaction volume by supplier, spending trends by department, or system access frequency by user are all within the scope of descriptive analytics. Diagnostic analytics investigates the cause of the situation. For example, if there is an unusual increase in payments to a particular supplier, it is examined whether this is due to a price increase, transaction splitting, authorization abuse, or weak control. Predictive analytics attempts to predict future risks based on past and present data. Directive analytics generates recommendations on what actions should be taken against the identified risks. Ilori et al. (2024) state that machine learning and predictive analytics techniques can be used to identify patterns, predict future risks, and detect anomalies.

One of the key contributions of data analytics to internal auditing is the shift from a sample-based approach to a more comprehensive one that analyzes nearly the entire transaction universe. In traditional auditing, auditors examine only a specific portion of the transaction

universe due to time and resource constraints. This can lead to some risky transactions being overlooked if they are not included in the sample. Data analytics, however, allows for the analysis of all or a very large portion of sales, purchasing, inventory, payroll, collections, payments, access management, and customer transaction data. Thus, the auditor can see not only errors in selected samples but also unusual transactions, recurring patterns, control deviations, and potential indicators of fraud within the entire dataset.

Audit analytics also strengthens the risk-based internal audit approach. The aim of risk-based internal audit is to direct audit resources to processes where the most significant risks for the organization are located. However, risk assessment may be incomplete if it relies solely on management statements, previous period findings, or general observations. Data analytics adds objective evidence at the transaction level to risk assessment. For example, unusual transaction times in the payment process, split payments to the same supplier, manual interventions, frequently canceled transactions, or recurring payment amounts close to authorization limits can be used as risk indicators. These indicators reveal not only individual transaction errors but also weaknesses in control design and control implementation. Ilori et al. (2024) state that advanced data analytics increases audit efficiency and effectiveness by focusing audit efforts on high-risk areas.

Data governance is a fundamental building block of audit analytics . The reliability of analytical results depends on the accuracy, integrity, consistency, timeliness, and security of the data used. Incomplete, erroneous, duplicate, misclassified, or unauthorizedly modified data can lead to inaccurate audit results. This is particularly critical in fraud detection and risk scoring models. Erroneous data can cause legitimate transactions to appear fraudulent or genuine fraudulent transactions to be overlooked. Therefore, when applying data analytics in internal audit, data sanitization, data validation, data integration, data security, access authorization, and data retention policies must be clearly defined. Ilori et al. (2024) emphasize that strong data governance practices are necessary to ensure data accuracy, consistency, and reliability.

Audit analytics does not eliminate the role of internal auditors; rather, it makes the auditor's professional judgment more important. Analytical tools can reveal unusual relationships in data, but it is the auditor's responsibility to assess whether these anomalies are due to error, fraud, systemic exception, a legitimate difference arising from the company model, or a deficiency in control design. Therefore, data analytics should not be seen as a technology that replaces the internal auditor, but rather as a tool that expands the auditor's analytical capacity, strengthens audit evidence, and supports risk-driven decision-making.

At this point, the relationship between artificial intelligence and data analytics is particularly important. Artificial intelligence represents a more advanced stage of audit analytics. While data analytics reveals patterns in data, artificial intelligence can learn from these patterns, classify risky behaviors, predict future risks, and provide decision support to the auditor. Raza et al. (2025) state that AI-powered data analytics, anomaly detection, and predictive modeling tools enable auditors to work more effectively on large datasets and detect fraud risks earlier. This assessment demonstrates that audit analytics is not merely a technical data review method, but a strategic tool that reshapes the internal audit's capacity to generate assurance .

6.2. Using Big Data in Internal Audit

Big data refers to data sets that are difficult to manage and analyze with traditional data processing methods, and which stand out with their volume, speed, variety, and accuracy. From an internal audit perspective, big data does not simply mean the growth of accounting records. Big data is fed from many different sources such as transaction records, user access logs , customer behavior, supplier information, device data, geographic location data, social media content, external threat intelligence, market data, regulatory information, and system records. According to Iseal et al. (2025), big data in financial services consists of different sources such as transaction data, market data, customer behavior data, external data, and IoT /geographic

location data, and these data play a critical role in risk assessment and fraud detection.

The most significant contribution of big data utilization to internal audit is the ability to assess the organization's risk profile in a broader and more holistic manner. Corporate risks are not only visible in accounting records. Risks can also manifest in user access, transaction times, system logs , supplier behavior, customer complaints, inventory movements, employee transactions, and external environmental data. Therefore, internal audit should include not only financial data but also operational , behavioral, technological, and external data in its analysis. Ilori et al. (2024) state that integrating different data sources, including financial, operational , and external data, provides a more holistic view of the organization's risk profile.

Big data analytics is critical, especially in fraud detection and prevention. Fraud in digital transactions is often not immediately apparent in a single transaction. Fraudulent behavior can manifest as small, consistent, repetitive movements leaving fragmented traces across different systems, or actions hidden within the normal flow of transactions. Big data analytics can make these hidden relationships visible by bringing together data from different sources. According to Udeh et al. (2024), big data analytics can detect anomalies and suspicious activity by leveraging various data sources such as transaction logs , user behavior patterns, and external threat intelligence; it can also incorporate multidimensional indicators such as transaction history, geolocation, device fingerprinting, and biometric data into risk assessment models.

The use of big data in internal auditing helps uncover patterns that are difficult or impossible to detect using manual methods. For example, in a payment database containing millions of transactions, the presence of different suppliers linked to the same bank account, unusual transactions made by the same user outside of business hours, recurring payments just below approval limits, or sudden increases in transactions deviating from customer behavior may not be easily detected by manual methods. Emran and Rubel (2024) state that big data analytics can reveal hidden anomalies in large financial datasets,

and fraud indicators can be identified using machine learning techniques in cases where manual detection is practically impossible.

Timing is a critical element in big data implementation. Traditional auditing often works retrospectively; that is, it detects errors or fraud after they have occurred. However, in the digital transaction environment, risks can emerge instantly and quickly lead to financial loss, reputational damage, or regulatory sanctions. Therefore, big data analytics generates higher value for internal auditing when it provides real-time or near-real-time analysis capabilities. Samuel (2023) states that the combined use of artificial intelligence, cloud computing, and big data technologies provides real-time detection, scalability, and accuracy in financial fraud detection systems. Real-time analytics, rather than batch processing, offers the possibility of immediate intervention in suspicious transactions.

Cloud-based big data analytics is also important for internal auditing and fraud detection. Processing large volumes of transaction data in on-premises systems can require high infrastructure costs and technical capacity. Cloud infrastructures, on the other hand, offer a flexible and scalable structure for storing and processing big data, managing real-time data streams, and running machine learning models. According to Samuel (2023), cloud computing infrastructure provides a suitable architecture for processing large volumes of transaction and behavioral data, integrating different data sources, real-time data streaming, and implementing AI-based fraud detection models in a scalable manner.

However, the use of cloud-based big data also creates new security risks. Storing and processing sensitive financial data in a cloud environment can increase the risks of data breaches, unauthorized access, API vulnerabilities, insider threats, model manipulation, and data privacy. Samuel (2023) emphasizes that data breaches, insider threats, and API vulnerabilities are significant threat vectors in cloud-based fraud detection systems; and that the cloud environment must be carefully managed in terms of data transmission, access control, and algorithmic bias. Therefore, internal audits should evaluate not only the technical capabilities of cloud-based analytics systems, but also

their security architecture, access controls, data encryption practices, logging mechanisms , and third-party service provider risks.

Big data analytics can also be used in the development of risk scoring models. A risk scoring model is an analytical structure that assigns a risk level to specific transactions, user accounts, suppliers, customers, or processes. For example, a supplier being newly established, frequent changes in bank accounts, receiving high-value payments, transaction approvals being made by the same user, and receiving payments at unusual times can increase the risk score. Such models help the auditor determine which transactions should be examined first. Ilori , Nwosu , and Naiho (2024) state that risk scoring , scenario analysis, and continuous risk monitoring models help prioritize risks and understand the effects of different scenarios.

The combined use of big data analytics and artificial intelligence enhances risk management and fraud detection in financial services. Iseal et al. (2025), state that artificial intelligence can rapidly process large datasets to generate more accurate and timely decisions in the areas of credit risk, market risk, operational risk, and fraud detection; and that anomalies indicating fraudulent activity can be detected by analyzing transaction patterns and consumer behavior. From an internal audit perspective , this means the auditor not only identifies past operational errors but also anticipates how risks might evolve in the future.

The limitations of big data usage should also be considered. Data quality, data privacy, model explainability , false positive/false negative rates, and algorithmic bias are among the main limitations. Emran and Rubel (2024) state that data quality, privacy concerns, and the interpretability of machine learning models pose significant obstacles in big data analytics applications; incomplete or biased datasets can lead to erroneous predictions. Therefore, the use of big data should be considered not only as a technology investment, but also as an organizational transformation requiring data governance, ethical principles, model validation, and internal control discipline .

6.3. Artificial Intelligence Applications

Artificial intelligence (AI) is a set of technologies increasingly used in internal auditing for data analysis, risk detection, control assessment, identification of fraud indicators, compliance monitoring, and decision support processes. AI applications encompass various techniques such as machine learning, deep learning, natural language processing, expert systems, decision support systems, neural networks, robotic process automation, graphical analytics, and predictive analytics. According to Ghafar et al. (2024), AI has provided significant advancements in data analysis, risk detection, compliance monitoring, and decision-making processes in internal auditing; machine learning, natural language processing, and predictive analytics tools have contributed to the automation of repetitive audit tasks, anomaly detection, and increased audit accuracy.

The first application of artificial intelligence in internal auditing is automation. Repetitive processes such as invoice matching, data retrieval, document classification, reconciliation checks, scanning user authorization lists, pre-evaluation of checklists, and standard report generation can be automated with AI-powered tools. This automation shortens audit time, reduces the risk of manual errors, and allows auditors to focus on higher value-added analyses. Ghafar et al. (2024) state that AI enables auditors to focus on more strategic governance and decision-making tasks by automating routine audit activities such as data extraction and identifying potential risks.

Machine learning is one of the most widely used areas of artificial intelligence in internal auditing. Machine learning algorithms can recognize specific transaction patterns by learning from past data and detect anomalies in new transactions. From an auditing perspective, these techniques can be used for transaction classification, financial statement analysis, identification of anomalous values, estimation of fraud risk, and prediction of control weaknesses. Ansari et al. (2025) state that artificial intelligence techniques such as machine learning, natural language processing, graphical analytics, and real-time data processing have significant potential in identifying complex, nonlinear, and evolving fraud behaviors.

Deep learning and neural networks are particularly important in internal auditing due to their capacity to analyze nonlinear relationships in large and complex datasets. These techniques can identify complex patterns that cannot be detected with simple rule sets. For example, transactions that occur at different times and from different accounts, and which appear normal individually, may indicate a fraudulent transaction chain when evaluated together. Bello and Olufemi (2024) state that deep learning methods, especially techniques such as CNN and RNN, can detect fraudulent patterns that are undetectable by traditional methods by analyzing transaction sequences, time series, and complex data patterns.

Natural language processing is a key area that enables artificial intelligence to analyze text-based data. In internal auditing, natural language processing can be used to examine contracts, emails, whistleblower reports, customer complaints, management statements, policy documents, audit reports, and financial statements. According to Bello and Olufemi (2024), natural language processing techniques can identify suspicious language patterns, keywords, and expressions that may indicate fraudulent intent by analyzing text data such as emails, chat messages, and transaction descriptions. This allows internal auditing to generate audit evidence not only from numerical data but also from unstructured data sources .

Qatawneh (2024) study also emphasizes the importance of natural language processing in the relationship between artificial intelligence, auditing, and fraud detection. The study states that AI-assisted auditing processes in accounting information systems are effective in data collection, data analysis, risk assessment, fraud detection, and investigation processes; and that natural language processing plays a complementary role in this relationship (Qatawneh , 2024). This finding demonstrates that the use of artificial intelligence in internal auditing can be applied not only to structured accounting data but also to broader data fields such as text-based descriptions, documents, and communication records.

Graphical analytics is particularly important in artificial intelligence applications for identifying complex fraud networks. It analyzes the

relationships between individuals, companies, bank accounts, suppliers, customers, users, and transactions within a network structure. This method can be used to identify related-party transactions, hidden partnerships, conflicts of interest, supplier corruption, money laundering, and organized fraud schemes. (Ansari, Valipour , and Salehi, 2025) states that graphic-based artificial intelligence techniques produce powerful results in detecting complex and unusual financial fraud patterns; however, this effect becomes more significant when supported by strong internal control systems.

AI-powered decision support systems can provide analytical support to internal auditors in determining which areas to prioritize. These systems help define the scope of the audit by bringing together transaction data, historical findings, control results, risk indicators, and external data. Ghafar et al. (2024) state that decision support systems assist internal auditors in financial data analysis, risk identification, and the development of audit strategies; predictive analytics allow for focus on high-risk transactions or departments.

Artificial intelligence provides speed, scope, and predictive power to internal auditing; however, its results should not be accepted without question. AI models depend on the quality of the data used, the design of the model, the representativeness of the training data, and the internal control environment of the organization. Ansari et al. (2025) state that AI methods have strong analytical capabilities, but the level of reliable and actionable results they produce depends on the strength of the internal control mechanisms within the organization. Therefore, artificial intelligence applications should be used in conjunction with independent human judgment, robust data governance, model validation, and ethical oversight in internal auditing.

Raza et al. (2025) state that artificial intelligence is not merely an automation tool that speeds up processes in auditing; it is a strategic technology that transforms fraud detection, risk assessment, and assurance quality. The study indicates that AI-powered tools make significant contributions to anomaly detection, real-time risk assessment, and improving the reliability of financial reporting. In this respect , artificial intelligence is a transformative tool in internal auditing

that reduces mechanical testing and directs the auditor towards more analysis, interpretation, and professional judgment.

6.4. Continuous Transaction Testing

Continuous transaction testing involves monitoring and testing internal transactions within an organization using analytical methods, not only at the end of the period but also while the transaction is occurring or very close to its occurrence. Unlike the retrospective nature of traditional auditing, this approach offers a proactive assurance mechanism. In organizations with high transaction volumes, it is often impossible for internal auditing to examine all transactions using classical methods. Continuous transaction testing automatically monitors transactions through specific risk indicators and control rules, generates alerts in unusual situations, and enables the audit team to intervene in a timely manner.

Continuous transaction testing is based on real-time data analytics. Transaction data is continuously analyzed; exceeding defined thresholds, unusual behavioral patterns, authorization breaches, or control deviations are automatically flagged. Udeh et al. (2024) state that real-time fraud detection mechanisms monitor transactions in real time, identify suspicious activity, and enable rapid action to prevent fraud. This approach ensures that internal auditing goes beyond being merely a function that reports past errors.

Continuous transaction testing can be used particularly in payment, purchasing, sales, collections, payroll, inventory, and user access processes. For example, in the purchasing process, making numerous payments to the same supplier in a short period, invoice amounts clustered just below the approval limit, frequent changes to the supplier's bank account, or creating duplicate records with the same invoice number can be monitored using continuous testing rules. In the payroll process, making payments to departing employees, sending multiple employee payments to the same bank account, or unusual overtime records can be identified as risk indicators. In user access, high- risk system logins

outside of working hours, incompatible permissions, or violations of job separation can be included in continuous monitoring.

Real-time transaction testing is crucial not only for fraud detection but also for evaluating control effectiveness. Just because a control is defined in a system doesn't mean it's actually working effectively. For example, a payment approval limit might exist, but users could bypass it by splitting transactions. Similarly, an authorization matrix might be designed, but old authorizations might not be removed after a role change. Continuous transaction testing makes these types of control circumvention behaviors and discrepancies between control design and implementation visible.

Samuel (2023) states that while batch processing methods can offer valuable insights, they introduce delays; in contrast, real-time analytics enables fraudulent transactions to be detected as they occur.This finding demonstrates why continuous transaction testing is critical in internal auditing . Because if a fraudulent transaction is detected days or weeks later, financial loss may have already occurred; whereas real-time analysis allows for intervention before damage happens or escalates.

Continuous process testing requires closer collaboration between internal audit and risk management and compliance functions. It must be clearly defined to whom the alerts generated by the system will be sent, within what timeframe they will be reviewed, under what circumstances the process will be halted, under what circumstances additional approval will be requested, and which findings will be reported to the audit committee. Otherwise, the system will generate numerous alarms, but these alarms will not translate into action. This creates a risk that can be described as "alarm fatigue." If the audit team consistently encounters low-impact alerts, they may miss truly critical ones.

Ansari et al. (2025) state that AI-powered real-time analytics systems can identify anomalies as soon as they occur; however, the conversion of these rapid insights into actionable results depends on well-structured internal controls, clear escalation protocols, effective communication channels, and standard documentation practices. Therefore,

continuous process testing should be designed not merely as a technical monitoring system, but as an internal control tool integrated with corporate responsibility, authorization, tracking, and reporting mechanisms.

Raza et al. (2025) state that AI-powered audit applications enhance real-time risk assessment, reduce operational costs, and support compliance processes. This finding demonstrates that continuous process testing is not merely a post-fraud investigation tool; it is a proactive internal audit mechanism that enables the monitoring of risks through an early warning system. Thus, audit activities cease to be periodic and transform into a continuous and dynamic assurance process.

Continuous process testing also transforms internal audit reporting. Traditional reporting is typically prepared after the audit is completed. With continuous testing, however, the audit committee and senior management can monitor risk indicators via live dashboards. For example, high-risk payment alerts generated in the last 30 days, pending exception reviews, resolved findings, recurring control violations, and the riskiest processes can be reported regularly. Ilori et al. (2024) state that interactive dashboards and detailed reports can provide real-time insights and visual presentation of key metrics; automated alerts can be set up for key risk indicators.

In this respect, continuous process testing makes internal auditing more dynamic, preventive, and data-driven. However, for this transformation to be effective, the internal audit team needs to acquire data analytics expertise, establish strong coordination with the information technology unit, clearly share responsibilities with controllers, and integrate continuous monitoring results into the audit plan.

6.5. Fraud Detection Using Analytics

Fraud detection is one of the most critical use cases for data analytics and artificial intelligence in internal auditing. Fraud is often not immediately apparent on the documents themselves; it hides patterns in

the timing, amount, parties involved, approval flow, user behavior, or frequency of transactions. Therefore, document review and manual checks alone are insufficient for fraud detection. Data analytics helps identify unusual transaction patterns, relationships, and anomalies that may indicate fraudulent behavior.

One of the fundamental analytical techniques used in fraud detection is anomaly detection. Anomaly detection aims to identify situations that deviate from normal transaction behavior. For example, an employee approving a high-value payment during hours when they don't normally process transactions, a customer generating a large number of return transactions outside of their usual behavior, or a supplier receiving an unusual payment in a short period of time can be considered an anomaly. Emran and Rubel (2024) state that anomaly detection plays a significant role in identifying indicators of financial fraud within big data; techniques such as clustering, classification, and regression can be used for fraud detection.

Machine learning algorithms are an important tool in fraud detection. Supervised learning algorithms are trained on transaction data that has been labeled as fraudulent and non-fraudulent in the past. The model classifies new transactions according to these past patterns. Unsupervised learning algorithms, on the other hand, try to identify transactions that deviate from normal behavior without pre-labeled data. This approach is particularly important in identifying previously unknown or newly emerging types of fraud. Bello and Olufemi (2024) state that supervised learning models are used to identify fraudulent transactions by learning from past data; while unsupervised learning methods are useful for detecting outliers that do not conform to expected behavior and new fraud schemes.

Natural language processing is also becoming increasingly important in fraud detection. Some indicators of fraud are revealed not in numerical data, but in text. Emails, contracts, explanatory notes, transaction descriptions, customer complaints, and whistleblowing texts can contain important clues regarding fraud. For example, expressions that suggest pressure, vague statements, contradictory statements, unusual keywords, or language patterns characteristic of

fraudulent attempts can be analyzed using natural language processing techniques. Emran and Rubel (2024) state that natural language processing helps identify suspicious communications and fraudulent intent by analyzing unstructured data sources such as emails, contracts, and social media.

Qatawneh (2024), while examining the impact of artificial intelligence on auditing and fraud detection in accounting information systems, draws attention to the complementary role of natural language processing. The study states that AI-supported accounting information systems can be used in data collection, analysis, risk assessment, fraud detection, and investigation processes; and that natural language processing can contribute to identifying fraud indicators, especially from text-based data. This approach demonstrates that internal audit fraud detection should rely not only on accounting records but also on data sources such as internal correspondence, contracts, statements, and whistleblower reports.

Behavioral analysis is also important in analytical-based fraud detection. Behavioral analysis models the usual behavioral patterns of users or transaction parties and detects deviations from these patterns. For example, let's assume a user always uses the system at certain times and for certain types of transactions. If the same user suddenly logs into the system from a different location at night and performs a high-risk transaction, this behavior can be considered unusual. Udeh et al. (2024) state that suspicious activities can be identified by analyzing user behavioral patterns through data such as login times, browsing history, and purchasing behavior.

Another approach that can be used for fraud detection is network analysis. Network analysis examines the relationships between individuals, companies, bank accounts, transactions, and system users. This method can be particularly useful in complex types of fraud such as conflicts of interest, collusion, related-party transactions, supplier corruption, and money laundering. For example, the use of the same address, the same phone number, or the same bank account by different suppliers; the concentration of transactions approved by an employee in certain suppliers; or the management of multiple

customer accounts from the same device can be seen with network analysis. Ansari et al. (2025) state that graph-based artificial intelligence is powerful in detecting relational, transactional , and network-based anomalies; however, robust data validation and internal control structures are necessary for reliable results.

The use of analytical methods in fraud detection strengthens the proactive role of internal audit. Putra et al. (2022) state that internal audit, risk management, whistleblowing systems, and big data analytics should be considered together in terms of fraud prevention and the prevention of financial crime behavior. This perspective demonstrates that fraud detection is not limited to the technical analysis of the audit unit; it must also be supported by corporate risk management, ethical guidelines, whistleblowing mechanisms, data analytics, and a robust control environment.

One of the contributions of artificial intelligence in fraud detection is that it reduces false positives and allows for greater focus on genuine risk signals. Raza et al. (2025) state that auditors believe artificial intelligence detects anomalies better than manual methods, reduces false positives in fraud detection, and increases accuracy in identifying irregularities. In the study, the average score for the statement "AI detects anomalies better than manual methods" was 4.35. The average score for "AI improves accuracy in identifying irregularities" was 4.28, while the average score for "AI reduces false positives in fraud detection" was 4.12. These findings demonstrate that AI-powered fraud detection tools are seen as useful not only in theory but also by practicing auditors.

However, analytics-based fraud detection must be considered along with the risks of false positives and false negatives. A false positive is when the system flags a legitimate transaction as fraudulent. This can create unnecessary investigation burden and operational delays. A false negative is when the system fails to detect a genuine fraudulent transaction. This can lead to financial loss and reputational damage. Ilori et al. (2024) state that advanced data analytics can increase the effectiveness of fraud detection and reduce false positives and false

negatives; however, this requires data quality, security, model currency, and corporate governance.

Therefore, the use of analytics for fraud detection in internal audit should be viewed as a continuously updated modeling process. As fraud methods change, analytical rules, risk indicators, and models must also be updated. Audit findings, whistleblowing results, investigation reports, and operational feedback should be used in model training. In this way, internal audit becomes an organization that learns from past fraud cases and can detect new risks earlier.

6.6. Ethical Concerns and Artificial Intelligence Risks

While artificial intelligence and data analytics offer significant opportunities in internal auditing, they also present serious ethical, legal, and managerial risks. Ignoring these risks could mean that AI-powered audit systems, instead of providing assurance, may create new control weaknesses. Key risk areas include data privacy, data security, algorithmic bias, model explainability, accountability, weakened human oversight, excessive automation, skill shortages, and regulatory compliance issues.

The use of artificial intelligence and data analytics in internal auditing creates important opportunities for more comprehensive, timely, and risk-oriented assurance. However, these technologies also introduce ethical, operational, and regulatory risks that must be carefully governed. Since internal audit analytics may involve employee records, customer information, supplier data, financial transactions, access logs, behavioral indicators, and other sensitive business information, data privacy becomes one of the most critical concerns. Audit analytics should therefore be based on the principles of relevance, necessity, restricted access, secure storage, and controlled use of data. Emran and Rubel (2024) emphasize that data quality, privacy concerns, and model interpretability are among the major obstacles in big data analytics and artificial intelligence applications.

Algorithmic bias is another significant risk in AI-assisted auditing. Artificial intelligence models learn from historical data, and if that data is incomplete, inconsistent, unbalanced, or biased, the model may reproduce and even reinforce existing distortions. For example, if certain departments have historically been audited more frequently and have generated more findings, an algorithm may classify those departments as inherently riskier. Conversely, units that have been audited less frequently may appear less risky, even when they contain material control weaknesses. Iseal et al. (2025) note that data privacy, regulatory compliance, and algorithmic bias must be carefully considered when artificial intelligence and big data are used in financial services and risk-related applications.

Model explainability is also central to the reliability of AI-supported internal audit work. Internal audit findings must be understandable to management, process owners, the audit committee, and other relevant stakeholders. If an AI model classifies a transaction, user behavior, or process as high-risk, the auditor should be able to explain the indicators and logic behind that classification. Otherwise, the model output may have limited evidential value. Samuel (2023) discusses the importance of model interpretability, regulatory compliance, adversarial behavior, and security risks in cloud-based AI fraud detection systems, and highlights the need for explainable AI, secure computing techniques, and privacy-preserving methods for the ethical and reliable use of artificial intelligence.

The weakening of human oversight constitutes another important risk. Even when AI systems produce highly accurate outputs, they are not infallible. If auditors accept algorithmic results automatically without professional skepticism, audit judgment may become dependent on technology rather than supported by it. This risk is especially important in fraud detection because fraudsters may learn how automated systems operate and attempt to manipulate or bypass them. For this reason, AI-assisted auditing should be designed around a human-in-the-loop approach, where the final assessment and audit judgment remain the responsibility of the auditor.

The reliability of AI-based fraud detection also depends heavily on data quality and the strength of the internal control environment. Ansari et al. (2025) state that AI-based fraud detection methods are technically powerful; however, noisy, inconsistent, or biased data may undermine the reliability of algorithmic decisions and lead either to false positives or to missed fraud indicators. This finding indicates that artificial intelligence cannot operate as a substitute for internal control. Rather, it should function together with strong controls such as data validation, segregation of duties, audit trails, model validation, and continuous monitoring mechanisms.

Information overload is another practical challenge associated with artificial intelligence and big data systems. These technologies can generate large volumes of alerts, reports, dashboards, and risk indicators. If such outputs are not properly classified, filtered, and prioritized, auditors may face difficulty distinguishing critical exceptions from routine system noise. Ghafar et al. (2024) state that AI and big data processing have a dual effect for auditors: they enable more accurate analysis of large audit datasets, but they may also create information overload when data is not effectively organized.

The effective use of artificial intelligence and data analytics also requires a higher level of auditor competence. Classical audit knowledge alone is no longer sufficient for evaluating algorithmic outputs, analytical models, and technology-based control environments. Internal auditors need to develop competencies in data literacy, model logic, basic analytical methods, data quality assessment, algorithmic risk, and technology governance. Raza et al. (2025) identify algorithmic transparency, ethical dilemmas, and skills gaps as barriers that limit the full implementation of artificial intelligence in auditing. Accordingly, organizations should provide continuous training in data analytics, artificial intelligence, and digital risk management for internal audit teams.

Regulatory compliance is another major consideration in AI-enabled audit practices. AI-powered audit systems must operate in accordance with data protection rules, cybersecurity requirements, financial regulations, labor law, and ethical standards. Principles such as data

minimization, purpose limitation, access restriction, retention control, anonymization, and secure processing are especially important when personal data are used in audit analytics. Ghafar et al. (2024) argue that as artificial intelligence, blockchain, and other smart technologies become more embedded in audit practices, the need for compliance with cybersecurity, data protection, and general AI-related regulations will increase.

Empirical evidence also shows that auditors consider data privacy, security, ethics, and transparency to be central concerns in the use of artificial intelligence. Raza et al. (2025) report that "data privacy and security issues" received a high mean score of 4.10, followed by "ethical concerns regarding AI use" with a mean score of 4.02 and "lack of transparency in AI algorithms" with a mean score of 3.95. These findings suggest that AI-powered monitoring systems should be implemented with strong data security controls, ethical oversight, and algorithmic transparency. They also indicate that explainability should not be treated as a secondary technical feature, but as a fundamental requirement for audit reliability and accountability.

To manage these ethical and operational risks, the internal audit function should establish a clear governance framework for artificial intelligence applications. Such a framework should define model ownership, data ownership, access rights, validation frequency, error-rate monitoring, ethical assessment procedures, human oversight responsibilities, and reporting lines. The performance of AI models should be reviewed regularly, false positive and false negative rates should be measured, model outputs should be compared with actual audit findings, and models should be updated when necessary. In this way, artificial intelligence can support internal audit without weakening professional judgment, ethical responsibility, or the integrity of the audit process.

In conclusion, artificial intelligence and data analytics can enable internal audit to detect risks earlier, analyze the transaction universe more broadly, identify fraud indicators more systematically, and use audit resources more effectively. However, these technologies create new risks when used without ethical principles, data governance,

accountability , human judgment, and a strong internal control structure. Therefore, the success of artificial intelligence in internal audit depends not only on the power of the algorithm but also on the institution's control environment, data quality, auditor competence, and ethical governance capacity.

Chapter Summary

This section examines the impact of data analytics and artificial intelligence on internal audit. It emphasizes how audit analytics transforms internal audit from a function that merely checks past transactions into a structure that anticipates risks, detects unusual transaction patterns, and provides management with more timely assurance.

The chapter also discusses the contributions of big data usage to internal auditing. Big data analytics allows financial, operational , behavioral, and systemic data to be evaluated together; this helps in more comprehensively identifying indicators of fraud, control weaknesses, and high-risk transaction areas.

Artificial intelligence applications have been evaluated in terms of automation, risk assessment, natural language processing, machine learning, graphical analytics, and decision support systems in internal auditing. Furthermore, it has been explained how continuous process testing moves audit activities from periodic reviews to real-time monitoring and early warning mechanisms.

The chapter concludes by addressing ethical concerns and risks associated with the use of artificial intelligence and data analytics. Data privacy, algorithmic bias, model explainability , human oversight, information overload, skill shortages, and regulatory compliance issues are the main risk areas highlighted in this context. In conclusion, while data analytics and artificial intelligence have the potential to enhance the effectiveness of internal audit, they generate real value when used in conjunction with strong data governance, ethical principles, human judgment, and robust internal control structures.

PART III

INTERNAL AUDIT CASES AND APPLICATIONS

Chapter 7 – Revenue Recognition Manipulation

Case Study: Revenue Classification, Cut-off, and Collectibility Risk

Introduction

This case examines the audit risks related to the accuracy and periodic appropriateness of revenue records, sales performance, campaign invoices, exchange rate gains, and trade receivables of Nova Motors A.Ş. The company's significant shortfall in budgeted sales targets, the positive overall gross profit despite losses on some vehicle sales, and the prominence of campaign invoices as a profitability corrective factor create risk indicators that require careful consideration by the auditor.

The primary objective of this case is to demonstrate that revenue cannot be recorded solely through the issuance of invoices; it must be assessed in conjunction with the terms of the sale, delivery, transfer of ownership and risk, collectibility, contractual rights, and periodic compliance principles. In this context, the auditor should comprehensively examine the company's sales records, campaign revenues, exchange rate classifications, rent-a-car receivables, and customer reconciliation processes.

This case raises a discussion on the professional skepticism and audit procedures that auditors should apply, particularly regarding the risk of revenue manipulation, accrual-based income records, financial statement classifications, and the collectibility of accounts receivable.

7.1. Case Background

Nova Motors A.Ş. is a company operating in the automotive sector, working with a main dealership system and primarily engaged in vehicle sales, spare parts sales, service operations, and fleet sales. The company's business model includes large-scale fleet sales to rent -a-car companies in addition to traditional retail vehicle sales. These fleet sales have increased the company's sales volume; however, since a significant portion of sales are financed through credit, guarantees, foreign currency promissory notes, and long-term collection mechanisms, they pose serious risks to the company's revenue quality.

According to Nova Motors A.Ş.'s eight-month financial statements as of August 31, 2025, the company's gross sales were 7,956,558 USD, net sales were 7,949,682 USD, and cost of sales was 7,021,112 USD. Gross profit from sales was 928,570 USD. However, an examination of the sub-items of the income statement reveals that the company incurred a loss of 887,238 USD from its core operations, while ordinary income from other activities reached a significantly higher level of 5,204,286 USD. Despite this, the company closed the period with a net loss of 1,597,845 USD due to high financing expenses.

Although this table might initially suggest that the company's primary problem is financing costs, a more critical question from an audit perspective is whether the company's revenue and revenue-related income have been correctly classified. Could sales bonuses, campaign invoices, interest differences, exchange rate differences, and rediscount income have been used in a way that makes the company's ordinary sales performance appear stronger than it actually is?

The company's vehicle sales performance shows a significant deviation from budgeted figures. While 722 vehicles were budgeted for sale in the first eight months of 2025, actual sales reached only 278. This represents a reported negative deviation of approximately 160%. The economic crisis in Türkiye has significantly reduced sales volume; consequently, the company has become more reliant on campaign invoices, bonuses, interest, and other revenue streams to support sales revenue.

When examined in terms of vehicle sales, the selling price of many models was below cost. For example , gross losses were incurred in vehicle groups such as Focus , Mondeo , Transit, and Cargo. The report states that there was a total loss of 313,399 USD in vehicle sales, but thanks to campaign invoices totaling 371,183 USD issued to Ford Otosan, the profitability rate was brought to approximately 2%. This point is one of the most critical areas of revenue risk in this case. Because while the company's actual commercial sales performance generated a loss, the campaign invoices and other sales-related income improved the profit outlook.

Therefore, the case is not based on the classic principle of issuing fraudulent invoices or creating entirely fictitious sales; rather, it focuses on revenue classification, the accrual principle, collectibility, exchange rate gains, the quality of trade receivables, and the impact of incentive/premium income on the income statement .

7.2. Main Issue of the Case

Nova Motors A.Ş., while reviewing the interim financial statements as of August 31, 2025, identified unusual concentrations in revenue and revenue-related income. The company was found to be incurring losses from its core operations, but this was partially offset by other operating income and campaign invoices.

The main problem with monitoring the case is this:

Has Nova Motors A.Ş.accounted for its sales revenue and other sales-related income in the correct period, for the correct amount, and under the correct classification; or has the company's financial performance been presented as more positive than it actually is through campaign revenues, exchange rate gains, rediscount interest income, and receivables with poor collection capabilities?

To answer this question, the auditor should not only look at the sales amount in the income statement. Revenue auditing should be conducted in conjunction with sales contracts, delivery documents, invoice records, collection status, customer balances, accounts receivable aging,

return and discount records, exchange rate calculations, promotional invoices, and post-balance sheet collection controls.

7.3. Revenue Structure of the Company

Nova Motors A.Ş.'s revenue structure consists of the following main components.

Table 7. 1. Main Components of Nova Motors A.Ş.'s Revenue Structure

Income Item	**Amount (USD)**
Domestic sales	7,543,336
Other income	413,222
Sales returns	-1,791
Other discounts	-5,085
Net sales	7,949,682
Cost of sales	-7,021,112
Gross sales profit	928,570

According to this table, the company appears to be generating gross profit from sales. However, a closer look reveals that a significant portion of vehicle sales are generating losses, while spare parts and labor revenues are supporting gross profitability. The losses from vehicle sales have been offset by campaign invoices and sales incentives. This requires auditors to evaluate revenue not only by its recorded amount, but also by its underlying quality, collectibility, and sustainability.

The company's "Other Income" account shows an amount of 413,222 USD consisting of interest on sales, turnover and performance bonuses, special discounts , and sales incentive bonuses. Whether this income should be shown as part of sales revenue, as other operating income, or as a discount/ reduction adjustment is a critical accounting decision for the auditor.

7.4. Risk Indicators

Nova Motors A.Ş.'s revenue records, sales performance, campaign invoices, exchange rate gains, receivables collectibility, and reconciliation processes reveals the following risk indicators regarding the accuracy and periodic suitability of revenue:

- A large discrepancy between budgeted sales and actual sales.

Nova Motors A.Ş.budgeted 722 vehicle sales for the first eight months of the year, but only sold 278. This discrepancy could put pressure on company management to meet revenue targets. Companies with significant deviations from sales targets risk bringing revenue forward towards the end of the period, recording uncompleted sales, exaggerating sales incentives, or presenting transactions with poor collectibility as sales.

From an audit perspective, this situation raises several issues that require detailed examination:

The audit of revenue recognition should focus on whether the sale of 278 vehicles represents genuine and completed transactions. This requires verifying that the vehicles were physically delivered to customers and that ownership, together with the significant risks and rewards associated with the vehicles, was effectively transferred. Sales recorded near the period-end should be examined with particular skepticism, since they may be exposed to subsequent returns, cancellations, renegotiations, or restructuring arrangements. Furthermore, invoices related to sales campaigns and performance-based bonuses should be supported by actual sales data rather than management estimates or provisional calculations. Evaluating these matters enables the auditor to assess whether revenue has been recognized in the correct period and whether the reported sales figures faithfully represent the underlying economic transactions.

- **Positive Gross Profit Despite Losses on Vehicle Sales**

The detailed sales table shows that for many vehicle models, the selling price is below the cost of production. For example, the Focus. Ghia , Focus Amb 4D, Focus Gross losses were incurred in the Amb 5D, Mondeo 4D Ghia , Transit, and Cargo groups. Despite this, total gross sales profit was reported as 928,570 USD. This figure was significantly influenced by spare parts and labor costs, as well as campaign invoices. The auditor should verify whether the discounts and campaign revenues received from the manufacturer were actually earned, whether the accrual conditions were met, and whether they relate to the correct accounting period.

- **Profitability Adjustment Through Campaign Invoices**

The report states that a loss of 313,399 USD was incurred in vehicle sales, but a campaign invoice of 371,183 USD issued to Ford Otosan increased the profitability to 2%. While this information does not directly raise suspicion of revenue manipulation, it warrants questioning the economic nature of the revenues.

The auditor should make the following distinction: Are the campaign invoices issued in exchange for a genuine service, sales support, or contractual right? Or are they revenue records created at the end of the period to compensate for vehicle sales losses?

If campaign invoices are based on actual sales, contracts, manufacturer approval, and proof of payment, they can be recorded as revenue. However, if the amount is based on an estimate, has not been accepted by the counterparty, or the performance obligation has not been fulfilled, recording the revenue may be problematic in terms of prudence and accrual principles.

- **Unusually High Other Operating Income**

Nova Motors A.Ş.'s other operating income is 5,204,286 USD This amount represents approximately two-thirds of its net sales. Other

operating income includes 3,910,276 USD in exchange gains and 1,213,113 USD in rediscount interest income.

These accounting income items, rather than the company's core business performance, significantly affected the period's results. A common occurrence in revenue manipulation cases is the aggressive use of ancillary income items during periods of weak sales performance.

- **Classification of Exchange Rate Gains**

In previous years, exchange rate gains related to rent-a-car fleet sales financed through Ford Credit loans were recorded under the "Other Income" account within "Gross Sales." As of 2025, exchange rate gains arising from the current year began to be tracked under the foreign exchange gains account.This change represents a significant classification risk. Tracking transactions of the same economic nature in different accounts during different periods impairs the comparability of financial statements . Furthermore, including foreign exchange gains within gross sales may inflate the company's operational sales volume.

Therefore, the auditor should compare past and current period classifications and question the management's rationale for the change in accounting policy.

- **Weak Collectibility of Rent-a-Car Receivables**

The company's total risk from rent- a-car companies as of August 31, 2025, is 37,488,374 USD. Of this amount, 32,880,933 USD is classified as non-performing, while 4,607,441 USD is classified as performing.

The existence of substantial overdue or distressed receivables creates a significant risk regarding the quality of previously recognized revenue. Revenue recognition should be supported not only by formal invoicing, but also by a reasonable expectation that the economic benefits associated with the transaction will be realized. If customers have lost their repayment capacity, are involved in legal enforcement procedures, or have entered bankruptcy or restructuring processes,

the auditor should evaluate whether the carrying amount of the receivables remains recoverable and whether an impairment allowance should be recognized.

- **Lack of Written Reconciliation**

As of August 31, 2025, no written reconciliation was conducted with buyers and sellers, and the company only conducted reconciliations at the end of the year. This situation represents a significant control weakness in terms of the accuracy and existence of accounts receivable balances in the interim audit. The fact that trade receivables have reached a particularly high amount of 32,957,818 USD makes this lack of reconciliation even more critical.

Without accounts reconciliation, it becomes difficult to obtain sufficient and appropriate audit evidence regarding the accuracy of revenues. The auditor should send client verifications directly and apply alternative tests for any unanswered balances.

7.5. Potential Revenue Manipulation Scenario

The audit team, based on preliminary analytical review, has determined that Nova Motors A.Ş.may have inflated its financial performance through the following methods, rather than through direct fraudulent sales:

One potential revenue manipulation pattern relates to the use of promotional invoices and special manufacturer bonuses to compensate for loss-making vehicle sales. In this scenario, vehicles may be sold below cost, while gross profitability is subsequently improved through promotional invoices issued to the manufacturer. From an audit perspective, the critical issue is whether these additional revenues are supported by contractual terms, measurable performance obligations, and actual economic substance. If such revenues are not linked to verifiable performance or formally approved incentive arrangements, they may distort the company's reported profitability.

Another area requiring audit attention is the classification of sales-related income under the "Other Revenues" account. Items such as

sales incentive bonuses, special discounts, turnover bonuses, and interest accruals may appear to support revenue performance, particularly when they closely move in line with net sales. However, the auditor should distinguish between amounts that have been finalized and those that are based on estimates, accruals, or management assumptions. This distinction is important for assessing the reliability, timing, and quality of reported income.

The treatment of exchange rate gains may also affect the presentation of operating performance. If foreign exchange gains were previously included within gross sales, this may have resulted in an overstatement of core sales performance. Their subsequent presentation under foreign exchange gain accounts in the current period raises questions about consistency, comparability, and the effect of reclassification on financial statement interpretation. The auditor should therefore evaluate whether the classification of exchange rate gains reflects the economic nature of the transactions and whether changes in presentation have been adequately justified.

Receivables with weak collectibility represent another significant risk area. High-value overdue balances, particularly those arising from car rental companies or financially distressed customers, may reduce the economic quality of previously recognized revenue. Even if a sale has been recorded in accordance with formal documentation, the related income may be of low quality if the receivable is unlikely to be collected. The auditor should therefore assess whether adequate provisions have been recognized and whether the carrying amount of receivables reflects their recoverable value.

Revenue cut-off risk should also be considered, especially where sales targets have not been achieved by the end of the reporting period. Pressure to meet budgeted sales levels may encourage management to record period-end sales, campaign invoices, or other revenue items aggressively. For this reason, transactions recorded close to the period end, particularly August sales, manufacturer campaign invoices, and other revenue entries, should be tested in detail. The audit should focus on whether revenue recognition is supported by delivery evidence, contractual entitlement, collectibility, and proper period allocation.

7.6. Audit Procedures

7.6.1. Analytical Review Procedures

The audit team should first conduct an analytical review of sales, cost of sales, gross profit, other income, exchange gains, and discount interest income. Vehicle sales volumes should be compared monthly with the budget and previous periods. A sales volume of 278 units compared to a budget of 722 units necessitates that the auditor seek consistency between expected sales volume and accounted-for revenue.

In addition, gross profitability analyses should be conducted on a product basis. Vehicle-specific sales price, cost, and gross profit/loss information should be examined; models where sales are made at a loss should be identified. For models where sales are made at a loss, explanations should be obtained from management, and how these losses are offset by campaign invoices should be investigated.

7.6.2. Sales Cut-off Tests

The auditor should perform a cutoff test on sales records near the end of the period. Sales recorded in the last week of August should be specifically selected; invoice date, delivery note date, delivery receipt, license/transfer documents, customer acceptance, and collection information should be compared.

The purpose of this test is to determine whether sales of vehicles that have not yet been delivered or for which risk and ownership have not been transferred to the customer are being recorded. If there are vehicles for which an invoice has been issued but delivery has not taken place, these sales should be removed from the period's revenue or treated as deferred income.

7.6.3. Testing Campaign Invoices

Campaign invoices are a key audit area in this case. The auditor should examine the basis for the campaign invoice amounting to 371,183 USD. This includes reviewing contracts with the manufacturer,

campaign terms, sales targets, dealer support letters, reconciliations, and collection documents.

The following questions must be answered for each campaign invoice:

Was the campaign mentioned in the invoice actually implemented? Which vehicle models did the campaign cover? What calculation method was used to determine the invoice amount? Did the manufacturer accept this amount? Was the amount collected, or was the collection made after the balance sheet? Was the revenue entry made after the relevant performance obligation was completed?

If sufficient evidence cannot be provided to answer these questions, a revision entry for campaign revenue should be recommended.

7.6.4. Classification Test of Other Income

The other income account, amounting to 413,222 USD , should be examined in detail. Interest, turnover bonuses, performance bonuses, special discounts, and sales incentive bonuses included within this amount should be classified separately.

The auditor should assess whether the accounting classification is appropriate for each type of income. Some items should be reported within sales revenue, some as sales discount adjustments, and some as other operating income. Incorrect classification can present net sales or gross profit differently than they actually are.

7.6.5. Examination of Exchange Rate Gains

Exchange rate gains amount to a significant sum of 3,910,276 USD. The auditor should break down which transactions generated this amount. According to the information in the report, a significant portion of the exchange rate gains stems from rent -a-car receivables, receivables arising from guarantee payments, and foreign currency-denominated promissory notes.

As part of the audit procedure, the year-end valuation of foreign currency receivables, the exchange rate used, the exchange rate at the collection date, the method of calculating exchange rate differences, and the accounting records should be checked. Furthermore, the need for reclassification should be evaluated for comparative financial statement presentation purposes, as exchange rate gains were previously recorded under gross sales.

7.6.6. Verification of Trade Receivables

Nova Motors A.Ş.'s trade receivables amount to 32,957,818 USD. This figure is quite high compared to net sales. The auditor should apply external reconciliation procedures to verify the existence, accuracy, and collectibility of trade receivables.

First, positive reconciliation should be sent to customers with large balances. For customers who do not respond, alternative procedures should be applied. These include reviewing collection receipts, checking bank statements, matching invoices and delivery notes, reviewing contracts, and performing post-balance sheet collection checks.

7.6.7. Rent a Car Receivables and Allowance Test

The problematic risk arising from car rental companies is 32,880,933 USD. This amount is extremely important for the company's financial statements. The auditor should not directly accept the distinction between problematic and non-problematic risks made by management; for each client, the auditor should analyze the payment history, litigation status, enforcement proceedings, collateral status, value of pledged vehicles, and likelihood of collection.

The lawyer's letter is one of the essential pieces of evidence for understanding the legal status of these receivables. The file indicates that legal action has been initiated against many rent -a-car companies, vehicles have been seized, some vehicles have been sold through foreclosure, and some debtors have entered into debt settlement processes through the transfer of real estate or shares.

The auditor should not consider the mere initiation of legal proceedings sufficient. Legal proceedings may increase the likelihood of collection, but they do not guarantee full collection. Therefore, the current market value of the collateral, the physical condition of the vehicles, their salability , and their priority status as collateral should be tested.

7.6.8. Subsequent Collection Tests

In revenue and accounts receivable audits, subsequent c ollection test is of critical importance. The auditor should evaluate the collectibility of recorded receivables at the end of the period by examining collections made after August 31, 2025. Data as of September 30, 2025 can also be used for this purpose. The file shows that as of September 30, 2025, the total risk has decreased to 37,353,047 USD, but the problematic risk is still 33,009,369 USD.

This result indicates that there has been no significant improvement in the quality of receivables in the short term. Therefore, the auditor should seriously consider whether a provision needs to be made.

7.7. Findings, Auditor's Assessment, and Recommendations

Nova Motors A.Ş.'s financial data as of August 31, 2025, reveals significant audit risks in terms of the company's revenue structure, other income items, exchange rate gains, and trade receivables. In particular, sales performance significantly below budget, losses from vehicle sales, profitability largely supported by campaign and incentive income, and the high amount of non-performing loans necessitate detailed audit procedures regarding the accuracy, classification, periodicity, and collectibility of revenue.

Table 7. 2. Control Weaknesses and Audit Risk Indicators in Nova Motors A.Ş.'s Revenue Recognition and Reciavables Processes

	Finding	**Auditor's Assessment**	**Suggestion**
1	Sales performance fell far short of budget. The company had budgeted 722 vehicle sales for the first eight months of 2025, but only sold 278.	Significant deviations from sales targets have placed pressure on management to generate revenue. This increases the risk of bringing forward revenue towards the end of the period, aggressively recording campaign revenue, or carrying back transactions with poor collectibility.	Discrepancies between budget and actual sales should be analyzed regularly; management explanations should be sought for large deviations, and period-end sales should be subject to specific audit procedures.
2	Vehicle sales generated a loss, while campaign revenues offset the profitability. A loss of 313,399 USD was incurred in vehicle sales; however, a campaign invoice of 371,183 USD to the manufacturer brought the profitability to approximately 2%.	The fact that profitability is supported by campaign revenues rather than actual vehicle sales is an important indicator of oversight. Campaign revenues cannot be considered reliable without testing whether they are based on contracts, actual sales, campaign terms, and counterparty acceptance.	Separate control files should be created for campaign and incentive revenues; each revenue record should be supported by a contract, campaign announcement, sales list, calculation table, counterparty approval, and receipt.
3	Other income has a significant impact on revenue. This other income, amounting to 413,222 USD, consists of interest, turnover and performance bonuses, special discounts , and sales incentive bonuses.	The auditor should determine whether these items should be classified as revenue, other operating income, discount adjustments, or financial income. Incorrect classification may misstate gross sales profit and operating performance.	Clear accounting policies should be defined for revenue, other operating income, interest on deferred payments, turnover bonuses, campaign support, special discounts, and sales incentive income.
4	There is a classification risk in exchange rate gains. In the past, some exchange rate gains were recorded under gross sales, but in the current period they have started to be tracked under the foreign exchange gains account.	This situation undermines accounting policy consistency and the comparability of financial statements . Foreign exchange gains should be separated from operational sales performance.	Exchange rate gains should be separated from gross sales and recorded in exchange rate profit or financial income accounts in accordance with their economic nature. Necessary reclassification explanations should be provided.

5	A significant portion of trade receivables are non-performing. As of August 31, 2025, the total risk arising from rent-a-car companies is 37,488,374 USD. Of this, 32,880,933 USD is classified as non-performing.	The collectibility of revenue is at serious risk. Customers experiencing payment difficulties, legal proceedings, vehicle seizure through foreclosure, and attempts to settle debts through real estate/share transfers are making the quality of past sales questionable.	Non-performing loans should be analyzed on a customer-by-customer basis; provisions should be made considering the remaining debt, collateral, value of pledged vehicles, enforcement status, collection history, and legal risks.
6	No written reconciliation was conducted during the interim period. The company only conducts written reconciliations with buyers and sellers at the end of the year. As of August 31, 2025, there are no written reconciliations for significant customer balances.	The lack of interim reconciliation makes it difficult to obtain sufficient audit evidence regarding the existence, accuracy, and collectibility of receivables. This represents a significant control weakness, particularly for high-backup and problematic customers.	Written reconciliations should be conducted quarterly for high-balance customers, non-performing loans, and rent -a-car companies. Reconciliation differences should be reported regularly and monitored by management.
7	Sales closing controls are not sufficiently visible. The delivery and customer acceptance processes for vehicles invoiced near the end of the period are not also monitored.	Recording revenue from vehicles for which invoices have been issued but delivery has not been completed creates a risk of error in terms of periodicity and realization principles. This situation may result in revenue being recorded before the relevant period.	Sales closing tests should be included in the internal control process; vehicles invoiced but not delivered should be automatically reported at the end of the period. Delivery documents and customer acceptance should be required before sales registration.

Overall, the risk of revenue manipulation at Nova Motors A.Ş. focuses more on the classification, accrual timing, and collectibility of revenues rather than directly on fraudulent sales. While the company's vehicle sales generated losses, campaign invoices, sales incentives, turnover bonuses, interest on deferred payments, and exchange rate gains supported the financial outlook. This structure alone is not proof of manipulation; however, it is an indicator of high risk. For the auditor, the primary priority is to test whether these revenues were actually earned, reliably measured, accepted by the counterparty, and recorded in the correct period.

7.8. Instructor Notes

This case study is designed to help students evaluate revenue auditing not just through the question of "are there sales invoices?", but through a broader reading of financial statements. In the case of Nova Motors A.Ş., sales invoices and records may be available; however, the real audit risk lies in the economic content of these sales, their collectibility, classification, and their impact on the income statement.

Students should be expected to discuss the following points in particular:

The classification of campaign invoices is a central issue in evaluating the quality of revenue presentation. The auditor should assess whether such invoices represent genuine revenue arising from a contractual entitlement, a reduction in the cost of sales, or another form of operating income. If campaign invoices are directly linked to manufacturer support, sales incentives, or compensation for pricing discounts, their economic substance should be carefully examined before they are treated as revenue. Misclassification may overstate gross sales or distort gross profit, particularly where the underlying vehicle sales are loss-making.

The presentation of exchange rate gains within gross sales also requires critical assessment. Foreign exchange gains generally arise from currency movements rather than from the entity's core sales activity. Therefore, including them within gross sales may give financial statement users an inflated impression of operational sales performance. The auditor should evaluate whether the classification of exchange rate gains is consistent with the nature of the transactions and whether any reclassification between periods affects comparability, trend analysis, or users' interpretation of revenue quality.

Non-performing receivables weaken the reliability of previously recorded sales because they raise questions about collectibility and economic substance. A sale may be formally recorded when an invoice is issued or delivery is completed; however, if the related receivable cannot be collected, the quality of that revenue becomes questionable. The auditor should therefore examine whether recorded sales are supported not only by documentation, but also by reasonable expectations of collection. High levels of overdue or doubtful receivables

may indicate that past revenue recognition was aggressive or that credit risk was not adequately considered.

The failure to recognize provisions for problematic receivables may materially affect reported profit. If doubtful receivables remain in the financial statements without an adequate allowance, assets may be overstated and expenses may be understated. As a result, profit may appear higher than its economically sustainable level. The auditor should assess whether management has applied a reasonable and evidence-based provisioning policy, considering customer payment history, aging analysis, subsequent collections, disputes, guarantees, and other indicators of impairment.

The gap between budgeted and actual sales can create significant pressure on management and may increase the risk of revenue manipulation. When actual sales fall below targets, management may have incentives to accelerate revenue recognition, classify supporting income more aggressively, delay impairment recognition, or use campaign-related invoices and other income items to improve reported performance. For this reason, the auditor should treat substantial budget variances as a risk indicator and perform detailed procedures on period-end sales, incentive income, receivables, provisions, and revenue classification.

This case demonstrates that revenue manipulation doesn't always mean creating fictitious sales. Sometimes, manipulation manifests as recording genuine transactions in the wrong period, classifying them in the wrong account, aggressively retaining revenues with poor collectibility in financial statements, or overstating core business performance with ancillary income.

7.9. Discussion Questions

1. Why are Nova Motors A.Ş.'s sales of 278 units against a budget of 722 units considered a significant risk indicator from a revenue audit perspective?

2. How might the fact that profitability was artificially improved through promotional invoices despite losses in vehicle sales affect users of financial statements?
3. Should all other income amounting to 413,222 USD be considered related to revenue? What additional evidence should be required?
4. What auditing problem arises from showing exchange rate gains under gross sales in the past and under exchange rate profits in the current period?
5. How do problematic rent-a-car receivables affect the reliability of past sales records?
6. Which audit procedures can compensate for the lack of written interim agreements with buyers?
7. In this case, for which revenue items should the auditor recommend an adjustment entry?
8. If company management claims that campaign invoices are contractually based, what documents should the auditor request?
9. How can the difference between revenue manipulation and classification error be explained using this case study?
10. Under what conditions could this case be the subject of a qualified opinion or a paragraph highlighting certain issues in an independent audit report?

7.10. Conclusion

The Nova Motors A.Ş.case demonstrates that sales figures alone are insufficient for revenue auditing. The company's sales volume fell significantly below budget, resulting in losses on many vehicle sales; however, gross profitability was supported by campaign invoices and other income. Furthermore, high amounts of exchange rate gains, rediscount interest income, and problematic rent -a-car receivables created significant risk areas that could lead to misinterpretations of the financial statements by users.

The auditor's primary task is not merely to determine whether revenue has been recorded, but to verify whether it was actually earned, whether

it is collectible, whether it belongs to the correct period, and whether it has been classified in the correct account. This case demonstrates that revenue manipulation often manifests not as overt fraud, but through accounting classifications, accrual decisions, and collection assumptions.

Appendix 7.1. Audit Questionnaire

Nova Motors A.Ş. Revenue Audit Questionnaire

	Area of Control	Question	Objective / Audit Risk
1	Sales Completion	Are there any invoices, delivery notes, delivery receipts, and customer acceptance documents for the vehicle sales recorded during the period?	To test the risk of recording unrealized sales as revenue.
2	Periodicity	For sales recorded near the end of the period, do the delivery date and invoice date belong to the same period?	To identify the risk of premature revenue recording.
3	Risk and Ownership Transfer	Have the risks and ownership of the vehicles been transferred to the customer?	To avoid the risk of listing vehicles for sale that have only been invoiced but not yet delivered.
4	Sales Targets	Has management provided an explanation for the fact that only 278 actual sales were made compared to the budgeted 722 sales?	To assess whether there is pressure on management to increase revenue.
5	Gross Profitability	Has a comparison been made between sales price and cost on a vehicle-by-vehicle basis?	To see the impact of selling at a loss on profitability.
6	Sales at a Loss	Is there a management statement and approval mechanism in place for vehicle models sold at a loss?	Assessing the risk of unusual pricing and revenue manipulation.

	Area of Control	Question	Objective / Audit Risk
7	Campaign Invoices	Have the campaign invoices issued to the manufacturer been linked to the contract, campaign terms, and sales lists?	To test the risk of recording unrealized or undeserved campaign revenue.
8	Sales Incentives	Have the sales commissions, performance bonuses, special discounts, and sales incentives been approved in writing by the counterparty?	To reduce the risk of recording income based on estimations.
9	Other Income	Are the amounts in the "Other income" account broken down into detail?	Check the distinction between revenue, other operating income, and discount adjustment.
10	Classification	Are interest charges, campaign subsidies, and sales incentives classified correctly in the accounts?	Identifying the risk of misrepresenting net sales and gross profit.
11	Exchange Rate Gains	Have exchange rate gains been recorded under foreign exchange profits instead of gross sales?	To prevent operational sales performance from being presented as higher than it actually is.
12	Accounting Policy	Are the past and current classifications of exchange rate gains consistent?	Assessing the risk of comparability and consistency.
13	Rediscount Revenues	Have the rediscount interest incomes been recalculated using the rates, maturities, and document amounts employed?	To test the risk of erroneous calculation of financial income.

	Area of Control	**Question**	**Objective / Audit Risk**
14	Trade Receivables	Have positive reconciliation statements been sent for customers with large balances?	To verify the existence and accuracy of receivables.
15	Lack of Agreement	Given that the company only performs reconciliation at the end of the year, have alternative procedures been applied for interim balances?	To reduce the risk of insufficient external verification.
16	Rent -a-Car Receivables	Have the receivables from car rental companies been analyzed on a customer-by-customer basis, categorizing them as problematic or problem-free?	Identifying receivables with low collectibility.
17	Problematic Loans	Have provisions been calculated for receivables classified as problematic?	To identify the risk of overstating profits by failing to set aside provisions.
18	Legal Follow-up	Have the lawyer letters and enforcement files been reviewed for clients who are subject to legal proceedings?	Evaluating the possibility of legal collection.
19	Guarantees	Have the current values of collateral such as pledged vehicles, real estate, and stocks been determined?	To test whether the collateral is sufficient to cover the debt.
20	Post-Balance Sheet Collections	Have the collections made after the end of the period been checked against bank statements?	To verify the collectibility of receivables.

	Area of Control	Question	Objective / Audit Risk
21	Sales Returns	Have sales returns or cancellations that occurred after the period been reviewed?	To identify the risk of premature or inaccurate revenue recording.
22	Discounts	the sales discounts and promotional offers been approved by authorized personnel?	Assessing the risk of unauthorized price reductions and revenue errors.
23	Related Party Transactions	Have transactions with group companies been monitored separately and assessed for compliance with market conditions?	To test the risk of revenue manipulation through related parties.
24	Payment Terms	Have payment plans, loan agreements, and guarantee obligations been reviewed in fleet sales?	Understanding the economic essence of sales and collection risk.
25	Management Approval	Have the unusual income records and campaign invoices been approved by senior management?	To reduce the risk of unauthorized or unreliable income recording.
26	Document Integrity	Is there consistency between sales invoices, shipping documents, accounting records, and collection records?	Identifying the risk of unofficial corrections or missing documents.
27	Revenue Cut-off	Has a cutoff test been conducted by comparing pre- and post-period sales?	Testing the risk of recording income for the wrong period.

	Area of Control	**Question**	**Objective / Audit Risk**
28	Financial Statement Presentation	Are revenue, other income, exchange gains, and financing effects presented separately and clearly in the financial statements?	To prevent financial statement users from being misled.
29	Internal Control	Is there a control point between the accounting, sales, and collections departments before the sales record is created?	To reduce the risk of unauthorized or incomplete sales records.
30	Results Evaluation	Have any significant errors, classification mistakes, or missing provisions been identified in the revenue records?	To assess its impact on the audit opinion.

Chapter 8 – Digital Procurement Fraud

Case Study: Fictitious Vendors, ERP Manipulation, Duplicate Payments, and Control Weaknesses

Introduction

This case is an anonymized and adapted case study prepared for educational purposes. The company name, reporting period, amounts, supplier names, and transaction details have been rearranged for instructional use. Accordingly, the case does not aim to represent any specific company directly, but to illustrate fraud risks, transaction errors, and internal control weaknesses that may arise in digital procurement processes.

The analysis covers supplier records, ERP logs, invoice entries, service procurement documents, and payment transactions recorded during the financial year ended 31 December 2024. This reporting period is used because the suspicious supplier relationships, duplicate payment indicators, ERP record changes, and weaknesses in service delivery evidence discussed in the case relate to procurement activities carried out throughout the 2024 fiscal year.

The case examines digital procurement fraud risks at Meridian Trade A.Ş.by focusing on purchasing, supplier management, ERP authorization, invoice control, service procurement, and payment processes. Although the company conducts these processes through an ERP system, the case demonstrates that digitalization does not necessarily ensure an effective control environment. Fraudulent or suspicious suppliers, post-entry changes to ERP records, duplicate payment risks, insufficient evidence of service delivery, and the circumvention of approval limits through invoice splitting are therefore treated as key areas requiring audit attention.

The main purpose of the case is to show that digitalization alone cannot be equated with strong internal control. ERP systems may

improve transaction recording, accelerate approval workflows, and facilitate data generation. However, where segregation of duties, supplier verification, three-way matching, data quality controls, service acceptance documentation, and continuous monitoring mechanisms are weak, the system may allow erroneous or fraudulent transactions to be processed in a more structured and less visible manner.

In this context, the case enables students to evaluate the digital procurement process beyond conventional document verification. It encourages analysis of system authorizations, transaction flows, data analytics outputs, ERP log records, duplicate payment detection procedures, supplier master data management, and audit evidence related to service procurement.

8.1. Case Background

Meridian Trade A.Ş.is a medium-to-large scale foreign trade company operating in the fields of import, trade, warehouse management, and supplying goods to group companies. The company's core business model is based on the sale of imported commercial goods to group companies and, to a limited extent, to external customers. Operational processes consist of areas requiring intensive document and system control, such as import, inventory management, warehouse leasing, transportation, service procurement, supplier payments, and current account tracking.

Due to its growing transaction volume, the company began managing its purchasing, inventory, accounting, and payment processes through a single ERP system at the beginning of 2023. With the implementation of the ERP system, purchase requests, supplier approvals, invoice entries, goods receipt records, and payment approvals were transferred to a digital environment. However, significant control gaps emerged in the purchasing process due to the rapid implementation of the system, the inadequate design of the authorization matrix, and the continuation of old manual practices.

The company's operational structure includes substantial expenditures related to warehouse rentals, service procurement, transportation,

consulting, representation, and supplier-based payments. Since these areas involve recurring transactions and document-intensive processes, they require careful audit attention in terms of authorization, service delivery evidence, invoice accuracy, and payment controls.For example, case data indicate that warehouse rental expenses, transportation expenses, service purchases, and representation expenses are examined separately; some expenses are classified in incorrect accounts; and there are missing documents and decisions in some transactions. This structure creates a suitable risk base for digital procurement fraud in the case of Meridian Trade A.Ş.

8.2. Main Issue of the Case

During the examination of Meridian Trade A.Ş.'s purchasing and payment processes as part of the 2024 internal audit plan, an unusual concentration of payments to certain suppliers was detected. Although the initial investigation suggested the problem was only "missing documents in purchasing records," data analytics revealed four key risk areas:

1. Fictitious or suspicious supplier records
2. Manipulation of purchase order and invoice information in an ERP system.
3. Duplicate payments for the same invoice or the same service.
4. Weaknesses in separation of duties, supplier verification, and payment confirmation controls.

The internal audit team decided to investigate unusual transactions, focusing particularly on warehousing services, transportation costs, consulting services, representation expenses, and maintenance and repair bills.

8.3. High-Risk Transaction Areas and Control Weaknesses

An examination of Meridian Trade A.Ş.'s digital procurement and payment processes reveals that the risks do not stem solely from individual transaction errors; rather, they arise from a broader control weakness related to supplier master data management, ERP authorization structure, duplicate payment controls, document procedures in service procurements, and payment approval mechanisms. Therefore, suspicious transaction areas and control deficiencies should be evaluated together.

8.3.1. Fictitious or Suspicious Suppliers

At Meridian Trade A.Ş., the supplier registration process is managed through the ERP system. According to standard procedure, the following documents must be uploaded to the system in order to register a new supplier:

- Tax certificate
- Commercial registry information
- Bank account verification document
- Authorized signature circular
- Purchasing department approval
- Finance department control
- Compliance or internal control unit approval

However, during the audit procedures, it was found that some supplier records did not include the required supporting documents. The suppliers with incomplete documentation are presented in Table 8.1.

Table 8. 1. High-Risk Suppliers Identified Due to Incomplete Documentation

Supplier Name	**Service Type**	**Total Payment for 2024**	**Risk Indicator**
Delta Warehouse Services LLC	Warehouse support service	385,000 USD	Incomplete supplier file
Nova Logistics LLC	Shipping and loading	268,500 USD	Similarity in bank account information.
Orion Consulting LLC	Consulting and process support	142,000 USD	Service output is uncertain.

These three suppliers have the following characteristics in common:

- It was registered in the system by the same user.
- The supplier opening dates are very close together.
- Invoice descriptions are general and repetitive.
- Some invoices do not include a delivery receipt or service report.
- There are similarities in the bank account information.
- The same purchasing personnel were found to be consistently involved in the approval chain.

This situation suggests that a fictitious supplier may have been created during the purchasing process.

8.3.2. ERP Manipulation

Upon examination of the ERP system, it was found that some purchase orders had been subsequently altered. Normally, after a purchase order is created, the goods or services should be accepted, then the invoice should be entered into the system, and the payment approval process should begin. However, in some transactions, the process was reversed.

These findings indicate a weakness in ERP-based procurement controls and raise audit concerns regarding the authorization, timing, and validity of purchase transactions. The relevant examples are summarized in Table 8.2.

Table 8. 2. Procurement Transactions with Altered Purchase Orders and Irregular Process Sequence

Transaction No.	**Supplier**	**Order Date**	**Invoice Date**	**Date of Acceptance of Goods/Services**	**Amount**
PO-2481	Delta Warehouse Services LLC	14.03.2024	12.03.2024	18.03.2024	48,000 USD
PO-2529	Nova Logistics LLC	25.04.2024	22.04.2024	30.04.2024	36,500 USD
PO-2634	Orion Consulting LLC	10.06.2024	June 8, 2024	None	27,000 USD

This table includes transactions where the invoice date precedes the purchase order or where there is no service acceptance record. This indicates

that the purchase documents may have been generated later in the ERP system.

A more serious finding is that some orders were revised after payment confirmation was completed. For example, in order number PO-2481, the initial amount was 28,000 USD, but it was increased to 48,000 USD just before payment confirmation. System log records show that the user who made the change was a purchasing specialist, but this same person also had the authority to define suppliers.

This is a clear violation of the principle of separation of duties.

8.3.3. Duplicate Payment with the Same Invoice Number

Within the scope of ERP data analytics, invoice records were matched using key transaction fields, including invoice number, supplier name, invoice date, invoice amount, and bank account number. This analysis revealed duplicate payment exceptions involving invoices with identical or similar information. The relevant exceptions are presented in Table 8.3.

Table 8. 3. Duplicate Invoice Payments Identified Through ERP Data Analytics

Supplier	**Invoice No.**	**First Payment**	**Second Payment**	**Total Risk Amount**
Nova Logistics LLC	NL-2024-118	24,750 USD	24,750 USD	24,750 USD
Delta Warehouse Services LLC	DD-445	31,000 USD	31,000 USD	31,000 USD
Has Transport Services LLC	HT-908	17,400 USD	17,400 USD	17,400 USD
Orion Consulting LLC	OC-077	12,500 USD	12,500 USD	12,500 USD

Total risk of duplicate payments: 85,650 USD

While some of these payments had the exact same invoice number, in some transactions the invoice number was re-entered into the system with minor changes. For example:

- NL-2024-118
- NL/2024/118
- NL 2024 118

Because the ERP system did not standardize invoice number formats, it perceived these records as different invoices. This is a significant vulnerability stemming from a lack of system control.

8.3.4. Invoicing from Different Suppliers for the Same Service

When the internal audit team reviewed expenses related to warehouse services, it identified similar invoices with comparable descriptions issued by multiple suppliers for the same location during the same period. This finding raises audit concerns regarding the validity, necessity, and potential duplication of warehouse service expenses. The relevant invoice examples for the Istanbul main warehouse in March 2024 are presented in Table 8.4.

Table 8. 4. Potential Duplicate or Overlapping Warehouse Service Invoices

Supplier	**Explanation**	**Amount**
Delta Warehouse Services LLC	Warehouse support service for March	48,000 USD
Beta Warehouse Solutions LLC	Warehouse operations support for March	46,500 USD
Nova Logistics LLC	March loading and unloading support	22,000 USD

Although the invoice descriptions appear different, the scope of services significantly overlaps. The service acceptance forms do not clearly indicate which supplier performed which work. This suggests that the same service may have been invoiced repeatedly under different names.

The source report also shows that expenses such as warehouse rent, warehousing services, transportation, paper cutting services, and similar costs reach significant amounts. These types of expenses are, by their nature, repetitive, document-intensive, and susceptible to manipulation.

8.3.5. Control Weaknesses

- **Weak Supplier Opening Control**

Although document uploading appears mandatory during the supplier registration process at Meridian Trade A.Ş., the system allows supplier registration to be completed even without these documents. Therefore, the procedure exists on paper; however, there is no effective mandatory control mechanism within the ERP system.

Deficiencies identified:

- Tax information verification is not performed.
- Bank accounts are not automatically linked to supplier titles.
- The system does not prevent multiple suppliers from using the same bank account.
- Independent financial audits are not required for supplier registration.
- No additional approval is required to reactivate inactive suppliers.

This structure creates a fertile ground for fraudulent supplier schemes.

- **Lack of Separation of Duties**

One of the most significant control vulnerabilities is the ability of the same user to perform multiple critical operations simultaneously. The investigation revealed that some users had the following permissions concurrently:

- Creating a new supplier
- Changing the supplier's bank account.
- Creating a purchase order
- Changing the order amount
- Entering a goods/services receipt record
- Submitting invoice entries for approval.

Combining these tasks within the same person significantly increases the risk of errors and fraud. In the purchasing process, tasks should be separated into at least the following categories: request creation, purchase approval, goods/service acceptance, invoice verification, and payment approval.

- **Ineffectiveness of Three-Way Matching Control**

In a healthy purchasing process, three documents should be compared before payment is made:

1. Purchase order
2. Record of receipt of goods or services
3. Supplier invoice

At Meridian Trade A.Ş., this control theoretically exists within the ERP system. However, the system allows for a certain tolerance difference between the amounts. The tolerance limit was initially set at 3%, and later increased to 15% for some users.

Therefore, for example, a purchase order of 40,000 USD could be matched with an invoice of 46,000 USD and enter the payment

process. The high tolerance rate has led to the misuse of purchase amounts.

- **Lack of Duplicate Invoice Check Before Payment**

The ERP system issues a warning for records containing the exact same invoice number. However, the system fails to detect the following situations:

- Spacing differences
- Punctuation differen
- Slash differences
- Case sensitivity
- Minor changes in supplier names
- Registering different suppliers with the same bank account.
- Similar invoices with the same amount and the same date.

Therefore, while the system prevents simple repetitions, it cannot prevent manipulated duplicate invoice entries.

- **Weak Proof of Delivery in Service Procurement**

Physical verification is easier in the case of goods purchases due to the inventory entry process. However, verifying whether a service has actually been received is more difficult in areas such as consulting, warehouse support, transportation, maintenance and repair, and representation services.

The following deficiencies were observed in the procurement of services at Meridian Trade A.Ş.:

- Service acceptance forms contain general statements.
- Consultancy reports have not been uploaded to the system.
- The shipping services lack a matching information between vehicle license plate, delivery point, and consignment note.

- Warehouse support services do not have staff lists or work schedules.
- The purpose of representation and hospitality expenses is not always clear.

The source report included detailed examinations of areas such as representation expenses, travel expenses, rental expenses, consulting services, and warehousing services; it was found that some expenses were misclassified or lacked adequate documentation. Such areas are at high risk for digital procurement fraud.

8.4. Potential Digital Procurement Fraud Scenario

The findings in the Meridian Trade A.Ş.case should not be considered as isolated and independent indicators of error, but rather as parts of a systematic control weakness in the digital procurement process. The ERP system digitized the procurement, supplier management, invoice recording, and payment processes. However, the system's lack of a control-oriented design, weak application of the principle of separation of duties, data quality issues, insufficient proof of delivery in service procurements, and lack of continuous monitoring created a suitable risk environment for digital procurement fraud.

According to the possible scenario, some suppliers were registered in the ERP system without sufficient verification; the same or related users were able to perform critical operations such as supplier registration, purchase order creation, order amount modification, and invoice submission for approval. This situation increased the risk of creating fake or suspicious suppliers, recording invoices without receiving services, subsequently altering order amounts, and losing control of the payment process.

In this case, suppliers such as Delta Depo Hizmetleri LLC, Nova Logistics LLC, and Orion Consulting LLC were specifically identified as high-risk. Payments made to these suppliers require a detailed audit due to incomplete supplier files, similar bank account information, invoice descriptions containing general statements, insufficient proof of service

delivery, and the continuous involvement of the same purchasing personnel in the approval chain.

ERP log records also provide significant indicators supporting this scenario. It was observed that some purchase orders were modified just before payment confirmation, some supplier bank accounts were updated close to the payment date, some invoice entries were made outside of business hours, and some documents were uploaded to the system after payment confirmation. These findings suggest that transactions were not carried out in accordance with the usual purchasing flow and that document completion or record manipulation may have occurred on the system afterwards.

The risk of duplicate payments is also a significant element of the scenario. Because the ERP system can only capture invoice numbers that are identical, changes in spaces, slashes, punctuation, or formatting in the invoice numbers cause the system to perceive the same invoice as different records. Therefore, the risk of multiple payments for the same invoice or the same service arises.

The lack of solid proof of delivery in service procurements further increases the risk. In services such as consulting, warehouse support, transportation, and maintenance/repair, the absence of tangible output, service acceptance forms, work schedules, transport documents, or operation reports makes it difficult to verify whether the service was actually received. This situation creates the risk of billing for services that did not take place or whose scope is unclear.

Furthermore, the splitting of some invoices to remain below the 25,000 USD approval limit suggests that senior management approval may have been deliberately disabled. Recording invoices separately from the same supplier that exceed the approval limit in total, within a short period, creates a risk of overshooting through invoice splitting.

The high-risk transactions identified in the Meridian Trade A.Ş. case were grouped by risk category and transaction type. Table 8.5 summarizes the total high-risk transaction volume identified during the audit review.

Table 8. 5. Summary of High-Risk Transaction Volume Identified in the Meridian Trade A.Ş. Case

Risk Area	**Amount**
Payments to high-risk suppliers	795,500 USD
Transactions suspected of ERP manipulation	326,000 USD
Risk of duplicate payments	85,650 USD
Service invoices lacking documentation.	214,300 USD
Split invoices below the limit	148,600 USD
Total risky transaction volume	**1,570,050 USD**

This entire amount should not be considered outright fraud. However, when the lack of documentation, system log findings, violations of separation of duties, deficiencies in supplier verification, indicators of duplicate payments, and invoice splitting practices are considered together, it is clear that Meridian Trade A.Ş. has a serious control weakness in its purchasing and payment processes.

This scenario demonstrates that digitalization alone does not guarantee effective internal control. An ERP system may have accelerated and recorded transaction processes; however, if the control design is weak, the system can cease to be a tool for preventing fraud and instead become a platform where fraudulent or erroneous transactions are legitimized within the system.

Therefore, the fundamental recommendation for Meridian Trade A.Ş.is not only to digitize the procurement process, but also to transform it into a control-oriented structure that adheres to separation of duties, is supported by data analytics, and is strengthened with continuous monitoring mechanisms. Supplier master data management should be strengthened, the ERP authorization matrix should be restructured, duplicate payment algorithms should be established, a standard of proof should be created for service purchases, and risk indicators should be regularly monitored with a continuous audit panel.

8.5. Audit Procedures

The internal audit team at Meridian Trade A.Ş. followed the procedures below to investigate digital procurement fraud.

8.5.1 . Supplier Master Data Analysis

The supplier master data file was retrieved from the ERP system and the following checks were performed:

- Different suppliers with the same bank account
- Different suppliers registered under the same tax number.
- Suppliers with incomplete addresses or missing tax information.
- Suppliers who opened their businesses in the last 12 months and received high-value payments.
- Suppliers that were reactivated after being inactive.
- Supplier addresses that are similar to employee addresses.
- Bank accounts that are similar to employee IBANs.

The analysis identified 11 suppliers as high-risk. Of these, 4 were found to have significant missing documentation, 3 were created by the same purchasing staff, and 2 used the same bank branch and similar account information.

8.5.2. Invoice Re-analysis

Invoice records were analyzed according to the following criteria:

- Same invoice number
- Similar invoice number
- Same supplier + same amount + same date
- Same bank account + different suppliers
- Same explanation + recent payment

- Round-amount bills
- Invoices entered on weekends or outside of working hours

This analysis revealed a confirmed duplicate payment risk of USD 85,650 and a potential duplicate or overlapping service billing risk of USD 214,300.

8.5.3. ERP Log Review

The ERP system logs were examined and the following findings were obtained:

- Some purchase orders were modified just before payment confirmation.
- Some supplier bank accounts were updated shortly before the payment date.
- The same user both created a supplier account and generated a purchase order.
- Some invoice entries were made outside of business hours.
- Some documents were uploaded to the system after payment confirmation.

These findings raise the possibility of deliberate manipulation of the system.

8.5.4. Document and Contract Review

Contracts, bid forms, service acceptance reports, and payment documents belonging to high-risk suppliers were examined. The findings are as follows:

- Some suppliers do not have a quotation comparison form.
- Some service procurements are not supported by formal written contracts.
- Some contracts have been drawn up with retroactive dates.
- Some service acceptance forms are standard and contain the same wording.

- Some invoices do not clearly indicate the scope of the service.

This situation indicates that the purchasing process was documented but weak in terms of content.

8.5.5. Payment Confirmation Process Review

An examination of the payment process revealed that invoices, particularly those below USD 25,000, were subject to less scrutiny. This finding indicates a potential control weakness in the payment approval process and suggests that certain invoices may have been deliberately split to remain below the approval threshold. The relevant examples are presented in Table 8.6.

Table 8. 6. Invoices Potentially Split Below the Payment Approval Threshold

Supplier	**Invoice Date**	**Invoice Amount**	**Explanation**
Orion Consulting LLC	June 5, 2024	24,800 USD	Process consulting
Orion Consulting LLC	June 6, 2024	24,600 USD	ERP support service
Orion Consulting LLC	June 7, 2024	24,900 USD	Purchasing process analysis

The total amount of these three invoices is USD 74,300. When considered together, they exceed the threshold requiring management approval. However, because the invoices were recorded separately, they remained subject to a lower approval level. This indicates a potential invoice splitting risk, whereby invoices may be divided to circumvent approval thresholds.

8.6. Findings, Auditor's Assessment, and Recommendations

An examination of Meridian Trade A.Ş.'s digital procurement and payment processes reveals that while the ERP system accelerates operational processes, it lacks sufficient robustness in terms of control design. Significant control weaknesses were identified, particularly in areas such

as supplier master data management, ERP authorization matrix, duplicate payment controls, and monitoring delivery proof and approval limits for service purchases. These findings indicate a high risk of fraudulent suppliers, duplicate payments, ERP manipulation, and undocumented service invoices within the company's procurement process.

Table 8. 7. Key Control Weaknesses in Meridian Trade A.Ş.'s Digital Procurement and Payment Processes

	Finding	**Auditor's Assessment**	**Suggestion**
1	There is a risk of fraudulent or suspicious suppliers. The investigation revealed that some suppliers were added to the ERP system without sufficient verification. Specifically, Delta Depo Hizmetleri LLC, Nova Logistics LLC, and Orion Consulting LLC were identified as high-risk suppliers. Total payments made to these suppliers amount to 795,500 USD.	While this entire amount is not considered fraudulent, a thorough investigation is required due to insufficient documentation and proof of service. Weak supplier verification processes increase the risks of paying fraudulent suppliers, conflicts of interest between employees and suppliers, fictitious service invoices, embezzlement of company assets, and misrepresentation of financial statements.	Supplier master data management should be strengthened. For new supplier registrations, tax identification number verification, bank account-compliance title matching, trade registry check, risky supplier list check, independent financial approval, and internal control/compliance unit approval should be made mandatory. The ERP system should not allow supplier registration to be activated without the uploading of mandatory documents.
2	The ERP authorization matrix is inadequate. It has been determined that some users have multiple critical authorizations, such as opening suppliers, creating orders, changing order amounts, and sending invoices for approval. The total value of transactions suspected of ERP manipulation is 326,000 USD.	Having the same user authorized to handle multiple critical operations indicates a violation of the principle of separation of duties. This increases the risks of creating unauthorized suppliers, subsequently increasing order amounts, recording fraudulent invoices, duplicate payments, and weakening the control trail.	The ERP authorization matrix needs to be redesigned. Purchase requests, supplier selection, supplier creation, goods/service acceptance, invoice registration, and payment approval should be separated among different individuals or departments. No single user should have the authority to both create suppliers and initiate the payment process.
3	Duplicate payment checks are ineffective. The system has	It is not sufficient for an ERP system to only perform checks	Duplicate payment algorithms should be implemented in the ERP

	been unable to detect some duplicate invoices due to differences in invoice number formats. Data analytics revealed a total risk of duplicate payments of 85,650 USD for the same or similar invoices.	based on an exact match of invoice numbers. Entering different invoice number formats can lead to double payments for the same service or goods, supplier reconciliation problems, incorrect cash outflows, and inflated expenses.	system. These include invoice number normalization, matching similar invoice numbers, checking for the same amount + same date + same supplier, checking for the same bank account + different supplier, checking for the same description + recent payment, and implementing warnings for recurring invoices with rounded amounts.
4	There is insufficient proof of delivery for services received. Objective documentation demonstrating actual service receipts has been found to be lacking for services such as warehouse support, consulting, maintenance and repair, and transportation. The total amount of service invoices requiring investigation due to insufficient documentation is 214,300 USD.	Service procurements have weaker physical proof of delivery compared to goods procurements. The absence of a service acceptance form, report, work schedule, or proof of delivery increases the risk of paying for services that were not rendered, exaggerating the scope of services, re-invoicing the same service through different suppliers, and concealing budget discrepancies.	A standard of evidence should be established for service procurements. Before payment is made for service invoices, the following documents should be requested: service acceptance form, service report, work schedule, proof of delivery, contract or order form, approval from the requesting unit, and documents demonstrating the service's relationship to the budget/activity. Payment should not be made for consulting services without concrete reports or outputs.
5	Approval limits were exceeded through invoice splitting. It was observed that invoices received from some suppliers were split in a way that	The practice of splitting invoices suggests that management approval may have been deliberately disabled. This weakens budget control and allows	Approval limits should be monitored in an aggregated manner. Similar invoices received from the same supplier within a short period should be combined

	kept them below the 25,000 USD payment approval limit. The total amount of invoices deemed to have been split below the limit is 148,600 USD.	fraudulent transactions to be concealed by breaking them down into smaller parts.	and evaluated by the system. For example, invoices received from the same supplier within 7 days and totaling more than 25,000 USD should be automatically forwarded to senior management for approval.
6	Purchase data is not monitored regularly. There is insufficient evidence to suggest that indicators such as fraudulent suppliers, duplicate payments, post-order amount changes, prepayment bank account changes, and limit splitting are regularly tracked.	The lack of internal auditing and continuous monitoring prevents the early detection of control vulnerabilities. While ERP systems generate transactions, if these transactions are not regularly analyzed for risk indicators, the system can become a platform for recording fraudulent transactions rather than preventing them.	A continuous audit panel should be established for the internal audit unit. Newly added suppliers, suppliers with incomplete documentation, suppliers using the same bank account, duplicate invoice candidates, post-order amount changes, prepayment bank account changes, split invoices below the limit, rounded-amount invoices, invoice entries outside of working hours, and invoices without service acceptance documents should be monitored monthly.

8.7. Instructor Notes

This case study is designed to encourage students to evaluate digitized purchasing processes not just through the lens of "Is there an ERP system?", but from a broader perspective of internal controls and fraud risk. In the case of Meridian Trade A.Ş., transactions are conducted through an ERP system; however, the primary audit risk is not the existence of the system itself, but rather whether the authorizations, controls, approval mechanisms, and data quality within the system are adequate.

Students should be expected to discuss the following points in particular:

The use of an ERP system does not automatically provide assurance over the purchasing process. Although ERP systems can strengthen transaction traceability, approval workflows, segregation of duties, and audit trails, their effectiveness depends on how the system is configured, monitored, and governed. If authorization rules are poorly designed, approval limits can be bypassed, supplier master data can be manipulated, or critical changes may remain undetected. Therefore, the auditor should not assume that the existence of an ERP system itself ensures control effectiveness. Instead, the audit should focus on whether ERP-based controls are properly designed, consistently applied, and regularly reviewed.

The risk of fraudulent suppliers should not be understood only as a problem of missing or incomplete supplier information. Although inadequate supplier master data is an important risk indicator, fraudulent supplier risk may also arise from employee-supplier relationships, similarities in bank account details, shared addresses, duplicate tax information, unusual payment patterns, or suppliers created shortly before large payments. For this reason, the auditor should evaluate not only whether supplier files are complete, but also whether supplier relationships, ownership links, bank account overlaps, and transaction behavior indicate potential conflict of interest or fictitious vendor risk.

A serious segregation of duties breach occurs when the same user has authority to create supplier accounts, generate purchase orders, change order amounts, and submit invoices for approval. These permissions allow one individual to control multiple critical stages of the procurement cycle. In such a case, the user may create a supplier, initiate a purchase, modify transaction values, and move the invoice through the approval process without sufficient independent review. This concentration of authority weakens preventive controls and creates an opportunity for fictitious suppliers, inflated invoices, unauthorized purchases, and concealment of irregular transactions.

Service purchases create additional audit evidence challenges because proof of delivery is usually less tangible than in goods purchases. In goods procurement, the auditor can examine purchase orders, goods receipt notes, warehouse records, delivery documents, and inventory movements. In service procurement, however, the evidence may consist only of service descriptions, consultant reports, e-mails, time sheets, or management confirmations. This makes it more difficult to determine whether the service was actually performed, whether the value charged was reasonable, and whether the invoice corresponds to a genuine business need. Therefore, service purchases require stronger documentation standards, clear service acceptance procedures, and independent confirmation of performance.

A large number of invoices below the approval threshold should not automatically be treated as a normal workflow. While such transactions may result from routine purchasing activity, they may also indicate invoice splitting designed to avoid higher-level approval. When several invoices are issued by the same supplier, on close dates, for similar services, and each remains just below the approval limit, the auditor should consider whether the transactions were artificially divided to circumvent control procedures. In this context, approval-limit testing should not be performed only on individual invoices; it should also include aggregated analysis by supplier, date range, department, project, and service type.

Overall, procurement auditing should examine whether the ERP environment supports real control discipline rather than merely

documenting transactions. The auditor should assess supplier master data controls, user authorization structures, segregation of duties, service delivery evidence, approval threshold compliance, and unusual transaction patterns together. This integrated approach enables the audit to identify not only formal control gaps, but also practical weaknesses that may allow procurement fraud, invoice manipulation, or circumvention of approval mechanisms.

This case demonstrates that digital purchasing fraud doesn't always manifest as overt deception. Sometimes, the risk of fraud or error arises through weak supplier verification, extensive ERP authorizations, missing service documentation, duplicate invoices that go undetected due to format discrepancies, and exceeding payment approval limits with fragmented invoices.

In the teaching process, students should not be expected to simply list the findings. For each finding, they should be expected to establish a connection between risk, financial impact, lack of control, audit procedure, and recommended corrective action. Therefore, the case is particularly suitable for discussing topics such as separation of duties, ERP controls, supplier master data management, duplicate payment analytics, and continuous audit dashboards in a practical way.

8.8. Discussion Questions

1. Why does the registration of some suppliers in the ERP system at Meridian Trade A.Ş., without sufficient verification create a significant risk of fraud?
2. What additional audit evidence should be requested to classify Delta Depo Hizmetleri LLC, Nova Logistics LLC, and Orion Consulting LLC as high-risk suppliers?
3. Could the entire 795,500 USD payment to high-risk suppliers be considered outright fraud? Why?
4. Which control principle is violated when the same user has the authority to open a supplier account, create an order,

modify the order amount, and submit an invoice for approval?

5. Which log records should an auditor examine for transactions suspected of ERP manipulation?
6. If duplicate payment checks fail due to differences in invoice number format, what data quality issue does this indicate?
7. In duplicate payment analysis, is matching only the invoice number sufficient? Which additional data fields should be compared?
8. Why does insufficient proof of delivery in service procurements create a higher audit risk compared to goods procurements?
9. What kind of fraud or oversight risk might a large number of invoices below the 25,000 USD approval limit indicate?
10. Why should using the same bank account by different suppliers be considered a red flag?
11. What should be the top three priority improvement actions for Meridian Trade A.Ş.?
12. Based on this case, what is the main lesson that digitalization has taught us in terms of internal control?

8.9. Conclusion

The Meridian Trade A.Ş.case clearly demonstrates that digitalization alone does not equate to effective internal control. While the company's purchasing and payment processes are managed through an ERP system, significant weaknesses exist in areas such as supplier master data management, authorization matrix, separation of duties, duplicate payment controls, service acceptance documents, and approval limits.

In this case, when payments to high-risk suppliers, transactions suspected of ERP manipulation, duplicate payment risk, service invoices with insufficient documentation, and invoices split below the limit are considered

together, the total risky transaction volume has been determined to be 1,570,050 USD. This entire amount should not be considered definitive fraud. However, this magnitude indicates a serious control weakness in the purchasing and payment process.

The auditor's primary task is not merely to determine whether transactions recorded in the ERP system have passed through the system, but also to test whether these transactions were initiated by authorized persons, whether they are based on actual delivery of goods or services, whether they have undergone appropriate approvals, whether they involve a risk of duplicate payments or invoice splitting, and whether they are supported by sufficient audit trails.

This case demonstrates that digital procurement fraud often manifests not as a single large fraudulent transaction, but through a combination of weak checkpoints within the system. When fraudulent or suspicious suppliers, broad user permissions, missing proof of service, data formatting issues, duplicate payment vulnerabilities, and below-threshold invoice splitting practices combine, the ERP system can transform from a tool that provides security into an environment where fraudulent or erroneous transactions can be concealed.

Therefore, the fundamental recommendation for Meridian Trade A.Ş. is not only to digitize the procurement process, but also to transform it into a control-oriented structure, compliant with separation of duties, supported by data analytics, and strengthened with continuous monitoring mechanisms. Centralizing supplier master data management, redesigning the ERP authorization matrix, establishing duplicate payment algorithms, creating a proof standard for service purchases, and monitoring risk indicators with a continuous audit dashboard should be key elements of this transformation.

Appendix 8.1. Audit Questionnaire

Meridian Trade A.Ş. Suspicious Transaction Areas and Digital Procurement Audit Questionnaire

	Area of Control	Question	Objective / Audit Risk
1	Supplier Opening	When opening new supplier accounts, have the tax registration certificate, trade registry record, bank account information, signature circular, and authorized person information been uploaded to the system?	Testing the risk of identifying suppliers with incomplete documentation and creating fraudulent suppliers.
2	Supplier Verification	Have the tax identification numbers, trade registry records, and business status of the new suppliers been independently verified?	To reduce the risk of making payments to fictitious or inactive suppliers.
3	Bank Account Check	Has a match been checked between the supplier's bank account and the supplier's name?	Identifying the risk of payments being made to bank accounts belonging to other individuals or businesses.
4	Same Bank Account	Has it been analyzed whether the same bank account is being used by multiple suppliers?	Identifying the risk of creating related, fraudulent, or shell suppliers.

	Area of Control	**Question**	**Objective / Audit Risk**
5	High-Risk Suppliers	Have detailed supplier reviews been conducted for Delta Depo Hizmetleri LLC, Nova Logistics LLC, and Orion Consulting LLC?	Evaluating the authenticity and validity of payments made to high-risk suppliers.
6	Supplier-Employee Relationship	Has an investigation been conducted to determine if there are any relationships between supplier partners, managers, or bank account holders and company employees?	To test for employee-supplier conflicts of interest and the risk of asset embezzlement.
7	Passive Suppliers	Is there a specific approval mechanism in place for reactivating passive suppliers that have been inactive for a long time?	To prevent the use of old or inactive supplier records for fraudulent transactions.
8	Supplier Master Data Changes	Have any changes to the supplier's name, address, tax number, or bank account been approved by authorized personnel?	Identifying the risk of unauthorized payments through critical master data changes.
9	ERP Authorization Matrix	Are user permissions aligned with job descriptions in the ERP system?	Assessing the risk of giving users excessive privileges outside of their assigned tasks.

	Area of Control	Question	Objective / Audit Risk
10	Separation of Duties	Does the same user have the authority to create a supplier account, generate orders, register invoices, and initiate the payment process?	To test the risk of error or fraud being committed and concealed due to a breach of the separation of duties.
11	Critical Users	Have users with critical ERP privileges been reviewed regularly?	Identifying unauthorized or over-authorized users.
12	Superuser Permissions	Are the actions of users with superuser or administrator privileges independently monitored?	To identify the risk of uncontrolled changes being made to the system and the weakening of the audit trail.
13	Purchase Order	Are purchase orders based on confirmed purchase requests?	To reduce the risk of creating orders that are not actually needed for the company.
14	Order Changes	Have any subsequent changes to order amount, quantity, or supplier information been tracked using log records?	To test the risk of fraudulent payments being made by subsequently altering order information.

	Area of Control	**Question**	**Objective / Audit Risk**
15	Pre-Invoice Order	Does the invoice date come after the purchase order date?	Identifying the risks of creating retroactive orders and subsequently completing documents.
16	Triple Match	Has a three-way matching process been established between the purchase order, the goods/services acceptance document, and the invoice?	To reduce the risk of paying for goods or services that have not been received.
17	Service Acceptance	Are service acceptance forms, service reports, work schedules, or output documents available for service procurements?	Testing the risk of paying for services that were not provided or cannot be proven.
18	Consulting Services	Are the consulting invoices supported by concrete reports, analyses, outputs, or delivery documents?	Identifying the risk of company resources being diverted through fictitious consulting invoices.
19	Warehousing and Logistics Services	Have warehouse support, transportation, and logistics services been verified with shipping documents, transport records, or operational reports?	To reduce the risk of overstating the scope of services or billing for services that were never rendered.

	Area of Control	Question	Objective / Audit Risk
20	Duplicate Invoice	Have records entered into the system with the same invoice number or similar invoice number formats been analyzed?	Testing the risk of multiple payments being made on the same invoice.
21	Similar Invoice Check	Have invoices with the same amount, same date, same supplier, or similar descriptions been compared?	To identify the risk of duplicate payments that the system might miss due to format differences.
22	Same Service Invoice	Has it been investigated whether the same service was re-billed through different suppliers?	Identifying the risk of multiple payments for the same service.
23	Prepayment Verification	Have the invoice, order, acceptance document, and bank account information been double-checked before payment is made?	To reduce the risk of erroneous, unauthorized, or duplicate payments.
24	Invoice Splitting	Have invoices received from the same supplier within a short period of time and just below the approval limit been analyzed?	Testing the risk of exceeding approval limits through invoice splitting.

	Area of Control	**Question**	**Objective / Audit Risk**
25	Approval Limit	Have aggregated checks been performed for numerous transactions that fell below the 25,000 USD approval limit?	Identifying the risk of circumventing top management approval through processes broken down into smaller parts.
26	Round Amounts	Have invoices with rounded consistency, frequent repetitions, or inadequate explanations also been investigated?	To identify the risk of unusual or artificially created transactional activity.
27	After-Hours Transactions	Have any supplier registrations, order changes, invoice entries, or payment transactions made outside of working hours been reported?	Identifying high-risk transactions that are outside of normal procedures.
28	ERP Log Records	Have the ERP log records related to supplier registration, bank account changes, order changes, and payment confirmation transactions been reviewed?	To verify who performed the transactions, when, and under what authority.
29	Log Integrity	Are there system controls in place to prevent the deletion or modification of ERP log records?	To maintain the reliability and traceability of digital audit evidence.

	Area of Control	Question	Objective / Audit Risk
30	Document Integrity	Is there consistency between the contract, order, acceptance document, invoice, payment order, and bank statement?	Testing the risk of payments being processed with incomplete or subsequently created documents.
31	Supplier Reconciliation	Have written agreements been made with high-risk and high-balance suppliers?	To verify the accuracy of outstanding balances and payment records.
32	Post-Balance Sheet Payments	Have payments made after the end of the period been matched with the relevant invoices and service documents?	To evaluate the accuracy of the debts and expenses recorded at the end of the period.
33	Related Party Risk	Has it been verified whether suppliers are related to company partners, directors, or employees?	Identifying the risk of resource transfer or conflicts of interest through related parties.
34	Data Quality	Are supplier names, invoice numbers, description fields, and bank accounts entered in a standard format?	To reduce the risk of automated controls failing due to poor data quality.

	Area of Control	**Question**	**Objective / Audit Risk**
35	Continuous Monitoring	Are new suppliers, suppliers with incomplete documentation, duplicate payment candidates, and below-limit split invoices regularly reported?	To enable the early detection of risky transactions.
36	Control Panel	Has a continuous audit panel been established for the internal audit unit regarding the purchasing and payment process?	To enable monthly or real-time monitoring of digital purchasing risks.
37	Management Approval	Have unusual supplier transactions, high-amount service invoices, and exceptional payments been approved by senior management?	To reduce the risk of critical transactions being executed without authorization.
38	Corrective Action	Has a corrective action plan been prepared for the detected duplicate payments, missing documents, or authorization violations?	To prevent the recurrence of control vulnerabilities.
39	Financial Impact	Have payments to high-risk suppliers, transactions suspected of ERP manipulation, duplicate payments, and invoices with missing documentation been assessed for financial impact?	To evaluate the impact of the findings on financial statements and cash outflow.

	Area of Control	Question	Objective / Audit Risk
40	Results Evaluation	Have any significant control lapses, indications of fraud, or financial misstatements been identified in the purchasing and payment process?	To determine whether the audit result requires reporting, investigation, or a record of correction.

Chapter 9 – Accounts Receivable and Collection Risks

Case Study: Receivables Aging, Collection Weaknesses, and Data Analytics Risk

Introduction

This case is an anonymized and adapted case study prepared for educational purposes. Company name, period information, amounts, customer names, and transaction details have been rearranged for instructional purposes. Therefore, the case is designed to discuss audit risks related to trade receivables, collection processes, accounts receivable aging, collateral adequacy, and the use of data analytics, rather than directly representing a specific company.

This case examines SAFER A.Ş.'s trade receivables and collection processes, including credit sales, check collection practices, customer guarantees, domestic and international customer reconciliations, and accounts receivable risk monitoring procedures.

While the company's receivables appear in its accounting records, the fundamental issue from an audit perspective is whether these receivables are economically collectible, whether their true age is accurately represented, and whether they are adequately supported by collateral.

The main objective of this case is to demonstrate that accounts receivable auditing is not simply about verifying whether customer balances are reflected in the records. The actual maturity of receivables, check renewals, returned and bounced checks, collateral coverage ratio, reconciliation deficiencies, post-balance sheet collections, and data analytics indicators must all be considered together.

This case study aims to have students analyze accounts receivable auditing in terms of assets, accuracy, valuation, collectibility, and provision risk. Specifically, it explores whether accounts receivable aging

reflects economic reality, the impact of problematic checks on collection quality, the relationship between collateral shortfalls and credit risk, and how ERP data can be used as an early warning mechanism.

9.1. Case Background

SAFER A.Ş. is a manufacturing company operating in the industrial wire sector. The company produces steel wire ropes, spring wire, tire wire, concrete wire, galvanized wire, and special industrial wire products, and sells them in both domestic and international markets. The company's sales model is largely based on credit sales. In domestic sales, the dealer network plays a significant role; in international sales, collection processes are carried out through group marketing companies, direct customers, and distributors.

SAFER A.Ş.'s receivables structure as of December 31, 2025 revealed three key risk areas that placed significant pressure on the company's cash flow:

1. The receivables aging report did not fully reflect economic reality;

2. The collection process had significant control weaknesses;

3. Data analytics was not used effectively to monitor receivables risk.

This case examines SAFER A.Ş.'s trade receivables and collection processes from an internal audit perspective, with particular focus on receivables aging manipulation, collection deficiencies, and the limited use of data analytics. Within this framework, the case evaluates audit procedures, findings, risk indicators, and recommendations.

9.2 . Main Issue of the Case

The main audit issue in the SAFER A.Ş. case is not merely whether trade receivables are recorded in the accounting system. The more critical question is whether these receivables reflect their true aging profile, whether they are collectible, whether they are adequately

supported by collateral, and whether they have been prudently valued in the financial statements.

The company's receivables portfolio includes significant amounts of credit sales, check collections, domestic and international customer balances, returned and bounced checks, and customers with collateral deficiencies. This structure necessitates an examination of receivables not only in terms of record accuracy but also in terms of credit risk, collection quality, cash flow impact, and the need for provisioning.

The fundamental control question of the case is whether SAFER A.Ş.'s trade receivables have been aged, verified, and valued in a manner that reflects their true collection risk, or whether the receivables portfolio has been presented as healthier than it actually is through check renewals, maturity extensions, problematic check transactions, reconciliation deficiencies, and insufficient collateral.

To answer this question, the auditor should not only look at customer current account balances. The first invoice date, first due date, check renewal history, returned or bounced check transactions, customer guarantees, reconciliation responses, post-balance sheet collections, and provisions for doubtful receivables should all be considered together.

9.3. General Overview of Trade Receivables

An examination of SAFER A.Ş.'s receivable accounts as of December 31, 2025, shows that the company has a significant short-term receivable balance, mainly arising from domestic and overseas buyers as well as promissory notes and post-dated checks. The composition of net short-term trade receivables is presented in Table 9.1.

Table 9.1. Composition of SAFER A.Ş.'s Net Short-Term Trade Receivables as of December 31, 2025

Account Item	Amount, USD
Domestic buyers	2,600,226
Overseas buyers	3,708,318

Public sector buyers	36,084
Other buyers	72
Total buyers	**6,344,700**
Promissory notes and post-dated checks	2,467,958
Accounts receivable discount (-)	(194,664)
Doubtful trade receivables	70,359
Provision for doubtful receivables (-)	(69,635)
Net short-term trade receivables	**8,618,718**

A significant portion of the company's total short-term trade receivables consists of accounts receivable from sales on credit, dealer receivables, foreign customers, and checks in the portfolio. While this structure supports the company's sales volume, it creates a financial statement item that requires careful monitoring in terms of collection risk, credit risk, and cash conversion cycle.

SAFER A.Ş. generally sets payment terms at 30, 60, and 90 days. However, investigations have revealed that some dealers are settling their due debts with new post-dated checks, some checks are being returned, and others are bouncing. This situation creates a risk area that could lead to a healthier-than-actual balance in accounts receivable aging reports.

9.4. High-Risk Process Areas and Control Weaknesses

An examination of SAFER A.Ş.'s trade receivables and collection processes reveals that the fundamental risk is not limited solely to whether receivables are recorded. The real audit risk lies in whether the true age of receivables is accurately tracked, whether check renewals and returned checks mask collection risk, whether customer guarantees adequately cover outstanding trade receivables, and whether domestic and international customer balances are verified with sufficient audit evidence.

Therefore, suspicious transaction areas and control weaknesses at SAFER A.Ş. should be evaluated under the following headings.

9.4.1. Risk of Accounts Receivable Aging Manipulation

Under normal conditions, receivables are monitored according to predefined aging ranges in order to assess collection risk and determine the need for doubtful receivable provisions. The standard aging ranges and corresponding risk levels are presented in Table 9.2.

Table 9.2. Standard Aging Ranges and Risk Levels for Trade Receivables

Aging Range	**Risk Level**
0–30 days	Low
31–60 days	Medium
61–90 days	High
91–180 days	Critical
181 days and older	Doubtful / overdue

Accounts receivable aging directly affects a company's collection quality, credit policy effectiveness, provisioning needs, and cash flow risk. Therefore, aging reports should be prepared not only based on accounting records but also on the economic reality of the receivable.

In the SAFER A.Ş. case, age manipulation does not directly mean fraudulent record keeping. However, certain practices can present the actual collectibility status of receivables as better than it actually is. Specifically, closing overdue receivables with new checks, replacing returned or bounced checks with new customer checks, and presenting the same receivable in the system with new due dates using different maturity dates are key indicators of this risk.

Some of the company's dealers are settling their due debts with post-dated checks instead of cash payments. This practice may appear in

accounting records as if the receivable has been closed or renewed. However, the economic risk of collection remains because the company has not collected the debt in cash; it has only received a new post-dated payment instrument to replace the old receivable.

Similarly, the exchange of returned or bounced checks for new customer checks, while explainable from a business perspective, is an area that requires careful monitoring from an auditing standpoint. Such transactions can conceal the true due date of receivables and collection delays.

Accounts receivable aging directly affects a company's collection quality, credit policy, liquidity position, and exposure to collection delays. The general overview of problematic check transactions at SAFER A.Ş. is presented in Table 9.3.

Table 9.3. Problematic Check Transactions of SAFER A.Ş. as of the First Quarter of 2026

Explanation	**Amount, USD**
Bounced checks	1,621,584
Returned checks	2,276,291
Bounced checks in the first quarter of 2026	559,743
2026 first quarter return checks	470,387
Total problematic check transactions	**4,928,005**

This magnitude indicates that the company has a high volume of check renewal and return transactions in its collection process. Therefore, the auditor should not only look at the current check maturity date or the last transaction date. For each receivable, the first sale date, first maturity date, first default date, last check date, and renewal count should be analyzed together.

In addition to its standard accounts receivable aging report, SAFER A.Ş. should prepare an economic aging report to assess not only the contractual aging of receivables but also their actual collectibility, legal status, and

credit risk. The key information to be included in this report is summarized in Table 9.4.

Table 9.4. Required Information for the Economic Aging Report of Trade Receivables

Data Field	Explanation
First invoice date	Date the debt arose
First due date	First payment obligation date
Deadline	History of the current collection method
Number of check renewals	How many times has the check been exchanged for the same debt?
Return/bounced check history	Customer's problematic payment history
Security status	Comparison of exposed risk with collateral.
The actual delay day	Delay from the first due date

This structure will allow us to track not only the accounting age of receivables but also their economic risk age.

9.4.2. Problematic Checks and Collection Quality Risk

At SAFER A.Ş., the collection process is mainly managed through coordination among the sales team, the accounting unit, and the finance department. However, the current structure does not provide a systematic, centralized, and data-driven control mechanism for monitoring overdue receivables, check renewals, collateral adequacy, and collection performance.

The main weaknesses in the collection process are as follows:

- Customer credit limits are not updated dynamically.
- The failure to conduct root cause analysis of returns and bounced checks on a customer-by-customer basis,
- Failure to regularly monitor the frequency of check renewals,

- The collection performance is not reported on a sales representative, customer, region, and product group basis.
- There are not enough restrictions on making new sales to customers with a history of problematic checks.

Problematic checks should not be considered merely a technical malfunction in the collection process. A bounced check is a significant warning sign regarding a customer's ability to pay or their financial discipline. While a returned check may be explained in some cases by business relationships, extended payment terms, or customer requests, a high volume and repeated return of checks indicate a weakening in the quality of collections.

Therefore, at SAFER A.Ş., problematic checks should be tracked in a separate collection risk database. For each problematic check, the customer name, initial sale date, check due date, reason for return or bounced check, whether a new check was received, the new check due date, whether interest was applied, sales representative, and collateral status should be recorded.

This structure will enable early detection of recurring collection problems with the same customers. Additionally, approval from the finance department or credit committee should be sought before making new sales to high-risk customers.

9.4.3. Lack of Agreement

SAFER A.Ş. is the inadequate level of customer reconciliation. Although reconciliation letters have been sent to a significant portion of domestic buyers, the response rate has remained limited.

As of December 31, 2025, the reconciliation status of SAFER A.Ş.'s domestic receivables was reviewed to assess the reliability, confirmation status, and potential collectibility risks of customer balances. The reconciliation results are summarized in Table 9.5.

Table 9.5. Reconciliation Status of SAFER A.Ş.'s Domestic Receivables as of December 31, 2025

Explanation	Amount, USD
Total domestic buyers	2,600,226
The amount for which an agreement response was received.	1,412,251
Amount for which no answer was received	1,187,975
Response rate	54%

The response rate of approximately 54% indicates that sufficient external verification evidence could not be obtained for all domestic receivables. For customers who could not be reached, alternative audit procedures should be applied; post-collection bank statements, shipping documents, sales contracts, invoice records, and customer correspondence should be examined.

The risk is higher for foreign receivables, as written account reconciliations had not been completed for foreign customer balances amounting to USD 3,708,318 as of December 31, 2025. The reconciliation status of foreign receivables is summarized in Table 9.6.

Table 9.6. Reconciliation Status of SAFER A.Ş.'s Foreign Receivables as of December 31, 2025

Creditors Group	Amount (USD)	Agreement Status
Overseas buyers	3,708,318	No written agreement has been reached.
Public sector buyers	36,084	No written agreement has been reached.

Lack of reconciliation in foreign receivables creates significant audit risk in terms of the existence, accuracy, and collectibility of the receivables. Furthermore, additional factors such as exchange rate differences, delivery disputes, quality problems, returns, transfer restrictions, and country risk must be considered in foreign currency receivables.

Therefore, SAFER A.Ş. must conduct written reconciliations at least twice a year for its international customers. Customers with high balances as of the balance sheet date, outstanding balances exceeding 90 days, exchange rate disputes, returns or quality problems, and those classified as related parties should be given priority for verification.

The priority customer groups for which reconciliation agreements should be obtained can be classified according to the criteria presented in Table 9.7.

Table 9.7. Risk-Based Prioritization Criteria for Receivables Reconciliation

Priority	**Criterion**
1. Priority	Balance exceeding 100,000 USD
2. Priority	Maturity exceeding 90 days
3. Priority	Customer with exchange rate dispute
4. Priority	Customer experiencing return or quality issues
5. Priority	Customer that is within the group or is a related party

Overall, reconciliation deficiencies weaken audit evidence regarding the accuracy of receivables. Therefore, the auditor should not accept unreconcilable balances solely on the basis of accounting records; they should support them with alternative verification procedures.

9.4.4. Collateral and Credit Control Weaknesses

SAFER A.Ş. receives various forms of collateral from its customers, including letters of guarantee, promissory notes, checks, foreign currency collateral, and mortgages. As of December 31, 2025, the general composition of collateral received by the company is summarized in Table 9.8.

Table 9.8. Composition of Collateral Received from SAFER A.Ş.'s Customers as of December 31, 2025

Type of Collateral	Amount (USD)
Letters of guarantee denominated in TL/USD	834,506
Promissory notes held as collateral	34,370
Checks held as collateral	76,810
Foreign currency collateral	551,300

Nevertheless, it has been observed that in some high-risk clients, the collateral does not cover the commercial risk.

While the total collateral amount appears significant, a customer-by-customer review reveals that for some high-risk customers, the collateral does not adequately cover the explicit commercial risk. Therefore, collateral should be evaluated not only based on the total amount but also in comparison with the existing accounts receivable risk on a customer-by-customer basis.

An examination of high-risk customers revealed a total collateral shortfall of 512,048 USD. This shortfall is particularly critical for customers with a history of bounced checks, unpaid checks, extended due dates, or check renewals. This is because, in the event of collection problems with these customers, the company's ability to secure its receivables may be limited.

This situation points to three key risks in the credit check process. First, customer credit limits are determined based on sales volume, and collection performance is not sufficiently considered. Second, collateral is not regularly renewed according to the current risk level. Third, new sales continue to be made to customers with insufficient collateral.

To mitigate these risks, SAFER A.Ş. should implement a structured credit control model covering customer risk assessment, credit limit

approval, collateral monitoring, receivables aging, reconciliation procedures, and collection follow-up. The recommended credit control model is summarized in Table 9.9.

Table 9.9. Recommended Credit Risk Management and Receivables Control Model for SAFER A.Ş.

Control	Explanation
Dynamic credit limit	Customer limits should be determined based on collection performance, not sales volume.
Collateral update	Guarantees must be updated at least twice a year.
Foreign currency collateral	For USD-denominated sales, USD collateral is preferred.
Automatic sales blocking	The system should stop new sales to customers with insufficient collateral.
Risk score	Bounced checks, returned checks, delays, and collateral rates should be scored together on a customer-by-customer basis.

Overall, collateral management at SAFER A.Ş. should not be limited to simply monitoring the total amount of collateral received. The auditor should assess whether the collateral covers the current commercial risk on a client-by-client basis, whether it is legally valid, its convertibility into cash, and its impact on the collectibility of receivables.

9.4.5. Doubtful Receivables and Provisioning Risk

As of December 31, 2025, SAFER A.Ş.'s doubtful trade receivables amounted to USD 70,359. A provision of USD 69,635 had been recognized for these receivables. The provision status of doubtful trade receivables is summarized in Table 9.10.

Table 9.10. Provision Status of SAFER A.Ş.'s Doubtful Trade Receivables as of December 31, 2025

Description	Amount (USD)
Doubtful trade receivables	70,359
Provision for doubtful trade receivables	69,635
Unprovided balance	724

At first glance, the provision ratio for doubtful receivables appears quite high. However, from an audit perspective, the real issue is not simply the adequacy of the provision allocated to existing doubtful receivables accounts. The more critical risk is the failure to identify receivables that, while not yet classified as doubtful, still pose an economic risk of non-collection.

At SAFER A.Ş., when check renewals, returned checks, bounced checks, customers with collateral deficiencies, and balances for which reconciliation responses cannot be obtained are considered together, it is seen that some receivables, although appearing as normal trade receivables in the accounting records, carry an economic collection risk. Therefore, provision analysis should not be performed only on amounts that have entered legal proceedings or have been transferred to the doubtful receivables account.

Additional provisions and impairment analysis should be performed, especially for the following groups of receivables:

- Receivables exceeding 90 days but renewed with a new check,
- Customers with insufficient collateral,
- Customers who have had more than one bounced check in the last 12 months,
- Customers whose return voucher volume is high relative to their sales volume,
- Customers who cannot receive a confirmation response,

- Customers with overseas receivables who have disputes regarding delivery, quality, returns, or exchange rate differences.

In this context, SAFER A.Ş.'s provisioning policy should be based not only on the legal status of the receivable but also on indicators such as the customer's payment history, check renewal frequency, collateral coverage ratio, number of days in arrears, reconciliation status, and post-balance sheet collection performance.

Overall, a high current provision for doubtful receivables is a positive indicator; however, this ratio does not eliminate the collection risk across the entire receivables portfolio. The auditor should separately analyze customer balances included in normal trade receivables but which have weakened economic collectibility and recommend additional provisions where necessary.

9.5. Potential Receivables Aging and Collection Risk Scenario

In the case of SAFER A.Ş., trade receivables appear to be present in the accounting records. However, the fundamental issue from an audit perspective is not whether these receivables are recorded, but rather whether the actual collection risk is accurately reflected in the financial statements. Considering the company's deferred sales model, check collection practices, payment extensions, returns and bounced checks, collateral deficiencies, and reconciliation shortcomings, there is a risk that the receivables portfolio appears healthier than it actually is.

In a possible scenario, some customers' overdue debts may have been renewed with new post-dated checks instead of being settled with cash collections. In this case, the accounting system appears as if the old receivable has been closed or replaced with a new, dated collection instrument. However, economically, the company has not received any cash collection, and the collection risk remains. This practice may cause receivables to appear younger and less risky in accounts receivable aging reports.

Similarly, replacing returned or bounced checks with new customer checks can mask collection risk. Even if a new check is technically received, the original due date, initial maturity date, and initial default date of the receivable remain unchanged. Therefore, the auditor should not consider the receivable new and valid simply by looking at the current check maturity date or the last transaction date.

Another important factor in this scenario is insufficient collateral. For some high-risk customers, insufficient existing collateral to cover the apparent commercial risk increases the likelihood of non-collection. Continuing sales to customers with a history of problematic checks and ongoing collateral deficiencies can increase the company's credit risk.

The lack of written reconciliation for foreign receivables is also a crucial part of the scenario. This lack of reconciliation makes it difficult to verify whether accounts receivable balances match customer records. It can also lead to delayed detection of risks such as exchange rate discrepancies, delivery disputes, quality issues, returns, or collection delays.

This structure does not directly mean that false receivables are being created. However, it increases the risk of receivables being presented as younger, safer, and more collectible than they actually are. This can lead to underestimation of doubtful receivables provisions, a better-than-expected collection performance, delayed detection of cash flow risks, and incorrect credit limit setting.

Therefore, the auditor's primary priority is not merely to verify whether receivables exist in the accounting records. For each significant receivable, the auditor should evaluate the first sale date, first maturity date, check renewal history, problematic check transactions, collateral coverage ratio, reconciliation status, and post-balance sheet collections together. In this way, the difference between the accounting age and the economic risk age of receivables can be revealed.

9.6. Audit Procedures, Data Analytics And Control Evaluation

The audit of SAFER A.Ş.'s trade receivables and collection process should not be limited to document verification alone; it should also include an assessment of receivables aging, collectibility, collateral adequacy, reconciliation results, subsequent collections, and data analytics indicators. Therefore, audit procedures should be designed to include document review, external verification, post-balance sheet collection testing, collateral analysis, and data analytics applications.

9.6.1. Document Examination Procedures

The auditor should first examine the documents underlying trade receivables. This includes comparing sales invoices with current account records, matching check receipt slips with bank collection records, and verifying how returned and bounced checks are reflected in customer accounts. Additionally, the basis for interest invoices, doubtful receivables records, provision calculations, and legal correspondence regarding receivables under legal pursuit should be reviewed.

The purpose of these procedures is to determine not only whether receivables exist in the records, but also whether they are based on an actual sales transaction, whether they belong to the correct customer, and whether they pose a risk in terms of collectability.

9.6.2. Verification Procedures

Positive reconciliation should be sent to domestic and international customers with high balances. International customers, in particular, those with receivables exceeding 90 days, customers with a history of problematic checks, and accounts with insufficient collateral should be prioritized for verification.

Alternative audit procedures should be applied for customers from whom a reconciliation response cannot be obtained. This includes reviewing post-balance sheet collections, bank statements, shipping

documents, customs documents, sales contracts, customer correspondence, and payment plans. For customers with discrepancies in reconciliation, the reason for the discrepancy should be analyzed in detail.

9.6.3. Balance Sheet Post Collection Tests

Post-balance sheet collection tests are critical for assessing the collectibility of trade receivables. The auditor should compare collections made after December 31, 2025, with bank statements and customer account activity.

Accounts receivable that were recorded at the end of the period but could not be collected after the balance sheet preparation, and which were renewed with new checks or restructured, should be examined separately. The need for provisions for doubtful receivables or impairment payments should be assessed for these receivables.

9.6.4. Security And Credit Limit Tests

The auditor should compare the commercial risk on a client-by-client basis with the available collateral. Letters of guarantee, promissory notes, checks, foreign currency collateral, and mortgages should be evaluated not only in terms of amount but also in terms of legal validity, current value, convertibility to cash, and capacity to cover the receivable.

New sales to customers with low collateral coverage ratios should also be examined. If a collateral shortfall, a history of problematic checks, and overdue receivables are observed together, these customers should be considered high-risk and an additional provisioning analysis should be performed.

9.6.5. Data Analytics Procedures

Certain receivables-related risks cannot be effectively detected through manual review alone. Therefore, data analytics procedures should be a fundamental part of the audit approach. The basic analytical tests that can be applied are summarized in Table 9.11.

Table 9.11. Basic Data Analytics Tests for Auditing Trade Receivables

Analytical Test	**Aim**
Aging analysis based on initial maturity date.	Determining the actual delay period of the receivable.
Check renewal frequency analysis	To determine how many times the same debt has been settled with a new check.
Analysis of problematic check rate	Measuring the frequency of returns and bounced checks on a customer basis.
Collateral gap analysis	Calculating the difference between commercial risk and available collateral.
Analysis of customers who did not receive a confirmation response.	Identifying balances with a high risk of external verification.
Sales increase – collection failure comparison	To see if the quality of collections deteriorates as sales volume increases.

These tests allow for the evaluation of receivables not only on a record basis, but also in terms of economic collection risk.

9.6.6. Audit Procedures, Data Analytics, and Control Evaluation

The audit should also evaluate SAFER A.Ş.'s internal control structure over accounts receivable and collection processes. The current review indicates that certain controls are not sufficiently robust. The main control weaknesses identified are summarized in Table 9.12.

Table 9.12. Key Control Weaknesses in SAFER A.Ş.'s Accounts Receivable and Collection Processes

Control Area	**Current Weakness**	**Risk**
Credit limits	It is not dynamically updated.	Risk of exceeding limits and collection issues.
Collateral management	Collateral does not always cover the exposed risk.	Collection loss
Agreement	Written agreement is missing for foreign receivables.	Balance accuracy risk
Check tracking	Returned and bounced checks are not subject to root cause analysis.	Continuous maturity renewal
Aging	The last transaction date is taken as the basis.	Aging risk of manipulation
reciprocity policy	Economic risk is not being given enough consideration.	Risk of insufficient reserves
Data analytics	There is no systematic early warning mechanism.	Late detection of risks

These weaknesses can make the company's accounts receivable portfolio appear healthier than it actually is. Therefore, accounts receivable management should be considered not only as an accounting and collection process, but also as a process encompassing credit risk, cash flow management, and financial statement valuation.

9.6.7. Receivables Risk Dashboard Recommendation

To ensure the regular monitoring of accounts receivable risk at SAFER A.Ş., an accounts receivable risk dashboard should be created within the ERP system. This dashboard should be regularly reviewed by finance management, sales management, and the internal audit department. The key indicators to be included in the dashboard are summarized in Table 9.13.

Table 9.13. ERP-Based Accounts Receivable Risk Dashboard and Monitoring Indicators

Indicator	**Aim**
DSO	Measuring the average collection time.
Overdue receivables	To track the share of overdue receivables within total receivables.
Problematic check ratio	Tracking the rate of returned, bounced, or repaid checks.
Collateral coverage ratio	Measuring the level at which collateral covers receivables on a customer-by-customer basis.
Renewal frequency	Analyzing check renewal frequency on a customer basis.
Disputed balances	Tracking unresolved or disputed receivables

By regularly monitoring these indicators, customers with collection risk can be identified earlier. Furthermore, the sales department can view a customer's outstanding balance, delays, check renewals, and collateral status before making a new sale.

Overall, the primary purpose of audit procedures at SAFER A.Ş. is not simply to verify accounts receivable. The auditor should assess whether trade receivables are presented accurately and prudently in the financial statements by considering the economic age of receivables, collection history, collateral adequacy, problematic check behavior, reconciliation status, and post-balance sheet collections.

9.7. Findings, Auditor's Assessment, and Recommendations

A review of SAFER A.Ş.'s accounts receivable and collection process reveals significant audit risks related to receivables aging, check renewals, collateral adequacy, international customer reconciliations, and the use of data analytics. Although the company uses ERP records to monitor accounts receivable and collection processes, the current reporting structure does not fully reflect the economic risk of receivables, the quality of collections, or customer-specific credit risk. Therefore, from the auditor's perspective, the fundamental risk is not merely whether the receivable exists in the accounting records, but whether it reflects its actual age, is collectible, is supported by adequate collateral, and is presented at its correct value in the financial statements.

Table 9.14. Key Audit Risk Indicators in SAFER A.Ş.'s Accounts Receivable and Collection Process

No	Finding	Auditor's Assessment	Suggestion
1	Accounts receivable aging does not fully reflect economic risk. At SAFER A.Ş., accounts receivable aging is tracked according to the last transaction date and the current check maturity date. However, renewed checks, returned checks, and maturity extensions can conceal the true age of the receivables.	The current aging structure does not indicate how long the receivable has been economically uncollectible. Renewing a check or extending its maturity can make the receivable appear new and problem-free. This can lead to a better-than-expected collection performance, an underestimation of the provisioning requirement, and a delayed identification of credit risk.	An aging report should be generated based on the first invoice date and first due date. The report should separately show the first invoice date, first due date, last check due date, number of check renewals, returned check history, and number of days in arrears.
2	The volume of problematic checks is high. When the data for the first quarters of 2025 and 2026 are considered together, the total problematic check transaction is 4,928,005 USD.	A high volume of problematic checks poses a significant risk to a company's collection quality. Check renewals, check returns, or maturity extensions indicate a lack of cash collection and a continued economic risk associated with the receivables. This weakens the ability to convert sales into collections and increases the risk of	Problematic checks should be scored on a customer-by-customer basis . Automatic sales blocks should be applied to customers who renew checks more than three times, have a history of bounced checks, or consistently postpone payment commitments. New sales should be subject to approval by the credit committee or finance director.

		impairment of trade receivables.	
3	Some clients have collateral shortfalls. Alke İnşaat, Çelsan A.Ş., and Hamdi Küçük have a total collateral shortfall of 512,048 USD in their accounts.	An insufficient collateral coverage ratio weakens a company's ability to secure its receivables in the event of non-collection. Especially with high-backup and delinquent customers, a collateral shortfall creates significant uncertainty regarding the collectibility of the receivable. This should be taken into account when calculating provisions and determining credit limits.	For customers with collateral coverage below 100%, new sales must be subject to approval by the finance director. Collateral should be monitored at its current value on a customer-by-customer basis; customers with insufficient collateral should be asked to provide additional collateral, bank guarantee letters, mortgages, or cash payments.
4	No written reconciliation was made for foreign receivables. The lack of written reconciliation for foreign receivables amounting to 3,708,318 USD represents a significant lack of verification.	The absence of written agreement on foreign receivables weakens the audit evidence regarding the existence, accuracy, and collectibility of these receivables. Foreign currency receivables may involve additional risks such as exchange rate differences, transfer restrictions , country risk, customer objections, and collection delays. Therefore, verifying foreign receivables solely through accounting records is insufficient.	Foreign customer reconciliation should be performed at least twice a year, before and after the balance sheet date. For high-balance foreign customers, a positive reconciliation method should be used; for balances for which no response is received, alternative verification should be carried out using post-collection bank statements, shipping documents, customs documents, contracts, and correspondence.
5	Data analytics procedures are inadequate. Although ERP records exist for accounts	The mere presence of data in an ERP system does not constitute sufficient control. Failure to use this data for customer-based risk scoring ,	A receivables risk dashboard should be added to the ERP system. The dashboard should regularly monitor DSO (Days Sales Outstanding),

	receivable and collection processes, the data is not effectively used for risk scoring and early warning mechanisms.	delay analysis, check renewal frequency, collateral coverage ratio, and disputed balance tracking can lead to delayed identification of problematic receivables. This prevents management from identifying collection risks in a timely manner.	overdue receivables, problematic check rate, collateral coverage rate, check renewal frequency, and unresolved/disputed receivables. Risk indicators should be reported on a customer basis, and automatic alerts should be generated when defined thresholds are exceeded.

Overall, the primary risk in SAFER A.Ş.'s receivables and collection process is not whether the receivables are recorded, but rather whether they are economically collectible. When check renewals, returned checks, maturity extensions, collateral deficiencies, and reconciliation shortcomings are considered together, it is evident that the company's receivables portfolio carries a significant level of credit and collection risk.

This structure alone is not proof of financial statement manipulation. However, it increases the risk of overstating receivables, underestimating provisions, and misrepresenting collection performance. For the auditor, the primary priority is to assess whether trade receivables are presented at fair value in the financial statements by considering the actual age of receivables, customers' payment capacity, collateral adequacy, check renewal behavior, and post-balance sheet collections.

9.8. Instructor Notes

This case study is designed to help students evaluate the accounts receivable and collection process not just based on the question of "are the receivables recorded?", but also considering the economic nature of the receivable, its collectibility, the adequacy of collateral, and its impact on the financial statements. In the case of SAFER A.Ş., the receivables appear to be recorded in the ERP system; however, the

real audit risk is whether the actual age of these receivables, the quality of collection, and the need for provisions have been accurately assessed.

Students should be expected to discuss the following points in particular:

The aging of accounts receivable should be assessed on the basis of the original invoice date and contractual due date rather than merely the most recent transaction date. If aging is calculated only from the last transaction, renewal, partial payment, or check replacement date, the receivable may appear more current than it actually is. From an audit perspective, the economic age of the receivable is more important than its accounting presentation. The auditor should therefore evaluate when the original sale occurred, when payment was initially due, and whether subsequent transactions have merely postponed the recognition of collection risk.

Check renewals and extensions of due dates may obscure the true credit risk of receivables. When overdue receivables are replaced with new checks or when due dates are repeatedly extended, the accounting records may show a formally renewed payment instrument, while the underlying customer risk remains unresolved. Such practices may delay the recognition of doubtful receivables and create the appearance of collectibility. The auditor should therefore distinguish between genuine collection and technical renewal, particularly where customers repeatedly replace checks without producing actual cash inflows.

A high volume of problematic checks is an important indicator of weaknesses in collection quality and cash flow reliability. Returned checks, unpaid checks, renewed checks, or checks repeatedly postponed may suggest that customers are experiencing financial difficulties or that the company's credit control procedures are insufficient. This situation may create liquidity pressure, weaken operating cash flows, and increase the likelihood of bad debt losses. From an audit perspective, problematic checks should be evaluated not only as isolated payment failures, but also as evidence of broader collection risk and possible impairment of receivables.

Continuing sales to customers with insufficient collateral may further increase credit risk. If a customer's outstanding balance exceeds the available collateral, or if collateral has not been updated in line with current exposure, the company may be extending credit without adequate protection. This practice may result in the accumulation of unsecured receivables and may increase the potential loss in the event of customer default. The auditor should therefore examine whether credit limits, collateral coverage, customer payment history, and ongoing sales decisions are monitored together.

The absence of written reconciliation for foreign receivables weakens the reliability of audit evidence. Foreign receivables may involve additional risks arising from exchange rate movements, cross-border communication difficulties, legal enforcement constraints, and differences in commercial practices. If written confirmations or reconciliations are not obtained from foreign customers, the auditor has limited independent evidence regarding the existence, accuracy, and collectibility of those balances. In such cases, alternative procedures such as subsequent collection testing, contract review, correspondence analysis, and management explanations should be carefully evaluated, but they may not fully replace direct written confirmation.

The lack of a risk dashboard or early warning mechanism in the ERP system should be evaluated as an internal control weakness, even if the underlying data exist in the system. Data alone does not create effective control unless it is converted into timely, relevant, and actionable information. If the ERP system contains aging data, collateral information, check status, customer limits, and collection history, but does not generate alerts for overdue balances, collateral deficits, repeated check renewals, or unusual collection delays, the organization is not using its information system effectively for risk monitoring. From an internal control perspective, this indicates a weakness in monitoring activities, information communication, and preventive risk management.

Overall, the audit of receivables and collection risks should focus not only on the recorded balance, but also on the economic substance of collection quality. The auditor should assess the original age of receivables, the frequency of check renewals, the volume of problematic

payment instruments, the adequacy of collateral, the reliability of foreign customer confirmations, and the effectiveness of ERP-based monitoring mechanisms together. This integrated approach enables the auditor to evaluate whether receivables are recoverable, whether provisions are adequate, and whether the company's credit control system provides timely warning of emerging collection risks.

This case demonstrates that simply verifying accounting records is insufficient in accounts receivable auditing. Accounts receivable may appear in the financial statements; however, factors such as repeated check renewals, extended due dates, customers providing insufficient collateral, inability to obtain written reconciliation, or weak post-balance sheet collections may indicate that these receivables carry an impairment risk.

During the teaching process, students should be expected to evaluate each finding at three levels. At the first level, the technical problem at the transaction or account level should be identified. For example, check renewal, collateral shortfall, or reconciliation deficiency. At the second level, the impact of this problem on the financial statements should be discussed. For example, insufficient provisions, overstating receivables, or concealing cash flow risk. At the third level, control recommendations should be developed. For example, an economic aging report, customer-based risk score, automated sales blocking, collateral coverage ratio monitoring, and accounts receivable risk dashboard .

This case is particularly suitable for the following course objectives:

- Evaluation of trade receivables in terms of asset, accuracy, and valuation claims.
- Separating the aging of receivables into technical aging and economic aging .
- Analyzing the impact of problematic checks on the quality of collections.
- Discussing the impact of collateral on the collectibility of receivables.

- Understanding the importance of external verification and alternative audit procedures in foreign receivables.
- ERP data could be used not only for record-keeping purposes but also for early warning and risk scoring .

Students should not be satisfied with the conclusion that "there are receivables" in the SAFER A.Ş. case. The more critical question is: How long have these receivables remained uncollectible, which customers are systematically renewing checks, do the collaterals cover the receivables, has written agreement been used to verify the accounts, and does post-balance sheet collection support the collectibility of these receivables?

Therefore, this case demonstrates the importance of professional skepticism in commercial receivables auditing. In particular, check renewals and extensions of maturity dates can mean postponing the collection problem. The auditor should not simply accept the receivable as new and sound based on the current check maturity date; they should analyze the collection process the receivable has undergone since its initial creation.

In conclusion, the SAFER A.Ş. case demonstrates that the fundamental objective in accounts receivable audit is not merely to determine whether an account receivable is recorded; it is to assess whether the receivable is economically collectible, whether it is supported by sufficient collateral, and whether it is presented at its correct value in the financial statements in accordance with the prudence principle.

9.9. Discussion Questions

1. Why might the receivables aging report at SAFER A.Ş. fail to accurately reflect the true collection risk?
2. What financial reporting risks arise from settling overdue receivables with new checks?
3. What is the difference between returned checks and bounced checks from an internal audit perspective?

4. What audit risks does the lack of written agreement on foreign receivables increase?
5. Is it appropriate to continue selling to customers with low collateral coverage ratios? Under what conditions should this be restricted?
6. What credit policy should be applied to customers with a high rate of problematic checks?
7. SAFER A.Ş. be determined solely based on receivables under legal pursuit, or should other indicators also be used?
8. Aging using data analytics How can manipulation be detected?
9. How can a conflict of objectives between the sales department and the finance department affect collection risk?
10. What are the three most critical control recommendations for SAFER A.Ş.?

9.10. Conclusion

SAFER A.Ş.'s trade accounts receivable and collection processes involve critical risks to the company's financial sustainability. Since the company's sales model is based on credit sales and collection by check, accounts receivable management should be treated not only as an accounting process but also as credit risk and cash flow management.

The key findings of the audit are as follows:

- Accounts receivable aging reports do not fully reflect economic risk.
- Renewed and returned checks weaken the quality of collections.
- The volume of problematic checks is high.
- Some clients have a collateral shortfall.

- No written agreement has been reached regarding foreign receivables.
- Data analytics procedures are not systematic.
- Provisions for doubtful receivables should not be assessed solely on receivables subject to legal proceedings; the economic risk of collection should also be considered.

Therefore, SAFER A.Ş. needs to transition to a more disciplined, data-driven, and control-based structure in its receivables management. In particular, the economic aging report , customer risk score , collateral adequacy analysis , check renewal tracking , and reconciliation monitoring system will reduce the company's collection risks.

Appendix 9.1. Audit Questionnaire

SAFER A.Ş. Accounts Receivable and Collection Risks Questionnaire

	Area of Control	**Question**	**Objective / Audit Risk**
1	Accounts Receivable Records	Are the trade receivables balances at the end of the period broken down by customer?	To test the accuracy and traceability of receivables on a customer-by-customer basis.
2	Accounts Receivable Aging	Is accounts receivable aging calculated solely based on the last transaction date, or also based on the first invoice and first due date?	Identifying the risk of concealing the debtor's true age.
3	Economic Aging	Has the aging report been generated based on the first invoice date and first due date?	To prevent the collection risk from appearing lower than it is due to renewed checks and extended due dates.
4	Extension of Maturity	Are receivables with extended maturities reported separately?	Assessing the risk of concealing collection difficulties through restructuring.
5	Check Renewals	Is it possible to track, on a customer-by-customer basis, how many times the same	Identifying customers with systematic collection problems.

	Area of Control	**Question**	**Objective / Audit Risk**
		customer has renewed a check?	
6	Refund Checks	Have the returned checks been analyzed based on customer, amount, date, and reason for return?	Identifying customers with poor collection quality and low payment capacity.
7	Problematic Check Volume	Have the problematic check transactions of 4,928,005 USD that occurred in the first quarters of 2025 and 2026 been broken down by customer?	To enable an assessment of the volume of problematic checks in terms of financial impact and customer risk.
8	Problematic Check Rate	Has the ratio of problematic checks to total collections or to the total check portfolio been calculated?	To measure the deterioration in collection quality.
9	Customer Risk Score	Have customers been scored based on check renewal frequency, days overdue, returned check history, and collateral adequacy?	To ensure that at-risk customers are identified at an early stage.
10	Sales Blockage	Is an automatic sales block applied to customers who renew	To avoid creating new credit risks for customers who

	Area of Control	**Question**	**Objective / Audit Risk**
		checks more than three times?	have ongoing collection problems.
11	Credit Limits	Are customer credit limits determined based on current financial status, payment history, and collateral level?	To reduce the risk of uncontrolled sales and non-payment of debts.
12	Exceeding the limit	Have sales to customers exceeding their credit limits also been approved?	Identifying the risk of unauthorized lending and the risk of increased receivables.
13	Collateral Tracking	Are the collaterals received on a customer basis tracked in terms of type, amount, maturity, and current value?	To assess the capacity of collateral to cover receivables.
14	Collateral Coverage Ratio	Has the collateral coverage ratio been calculated for each customer?	To test whether receivables are secured by collateral.
15	Collateral Deficiency	Have Alke İnşaat, Çelsan A.Ş., and Hamdi Küçük prepared an action plan for the total collateral deficit of 512,048	To reduce the risk of non-payment for customers with insufficient collateral.

	Area of Control	**Question**	**Objective / Audit Risk**
		USD in their accounts?	
16	New Sales Approval	Is it mandatory to approve new sales to customers whose collateral coverage ratio is below 100%?	To prevent uncontrolled sales to customers with insufficient collateral.
17	Post-Balance Sheet Collections	Have the collections made after the end of the period been checked against bank statements?	To verify the collectibility of receivables.
18	Overdue Receivables	Are overdue receivables classified by customer, number of days, and amount?	To determine the impact of overdue receivables on financial statements.
19	Correspondence Analysis	Have provisions been calculated for overdue receivables, receivables with insufficient collateral, or renewable checks?	Assessing the risk of overstating receivables.
20	Depreciation	Has an impairment assessment been conducted for receivables with poor collectibility?	To ensure that trade receivables are presented fairly in financial statements.
21	Domestic Agreement	Have positive reconciliation notices been	To verify the existence and accuracy

	Area of Control	**Question**	**Objective / Audit Risk**
		sent to domestic customers with large balances?	of receivables through external verification.
22	Foreign Agreement	Has a written agreement been reached for the foreign receivables amounting to 3,708,318 USD?	To provide audit evidence regarding the accuracy and collectibility of foreign receivables.
23	Agreement Responses	If discrepancies are found between the reconciliation responses and the accounting records, has a difference analysis been conducted?	To identify disputed or disagreed receivables.
24	Alternative Procedures	For customers from whom a confirmation response could not be obtained, have post-collection receipts, contracts, shipping documents, and correspondence been checked?	To compensate for the lack of external verification with alternative audit evidence.
25	Disputed Receivables	Are receivables related to customer disputes, price differences, quality issues, or delivery discrepancies tracked separately?	To identify receivables that are uncertain to collect or that may become subject to litigation.

	Area of Control	**Question**	**Objective / Audit Risk**
26	Legal Follow-up	Have the lawyer's letters, enforcement files, and collection possibilities been reviewed for clients facing legal action?	Evaluating the collectibility of receivables in legal proceedings.
27	Currency Risk	Have the exchange rate effects on receivables denominated in foreign currency been correctly calculated and reflected in the financial statements?	Testing the risk of exchange rate error in foreign currency receivables.
28	Foreign Receivables Risk	Have country risk, transfer risk, and collection delay been assessed for international customers?	Identifying additional collection risks in foreign receivables.
29	Collection Performance	Has customer-specific collection performance been compared to previous periods?	Early detection of deterioration in collection quality.
30	DSO	Has the mean time to collection, or DSO, been calculated and monitored on a period-by-period basis?	Measuring collection time delays and cash flow risk.
31	Overdue Receivables	Has the ratio of overdue receivables to	Assessing the risk level of the

	Area of Control	**Question**	**Objective / Audit Risk**
		total receivables been calculated?	accounts receivable portfolio.
32	Problematic Check Ratio	Is the problematic check rate monitored on a customer and period basis?	Measuring the deterioration in the quality of check collection.
33	Collateral Coverage Ratio	Is the collateral coverage ratio tracked on the dashboard on a customer-by-customer basis?	Identifying customers with insufficient collateral early on.
34	Renewal Frequency	Is the check renewal frequency automatically reported on a customer-by-customer basis?	Identifying customers whose payments are consistently delayed.
35	Disputed Balances	Are disputed or disagreed receivables tracked in a separate report?	To identify receivables whose accuracy and collection are uncertain.
36	ERP Data Quality	Are customer codes, due dates, check information, and collateral records kept in a standard format within the ERP system?	aging and risk scoring due to poor data quality .
37	Early Warning System	Does the ERP system have an automatic alert mechanism for delays, check renewals, collateral shortfalls, and	To ensure that collection risks are identified at an early stage.

	Area of Control	Question	Objective / Audit Risk
		reconciliation discrepancies?	
38	Management Reporting	Is the accounts receivable risk dashboard regularly reported to finance management, sales management, and senior management?	To ensure that accounts receivable risk is monitored in a timely manner by management.
39	Sales and Collection Connection	Does the sales unit check a customer's outstanding balance, overdue payments, check renewals, and collateral status before making a new sale?	To reduce the risk of making new sales to customers who have collection problems.
40	Results Evaluation	Have any significant collection risks, provision deficiencies, collateral shortfalls, or reconciliation deficiencies been identified in trade receivables?	To evaluate the impact of the findings on the financial statements, audit opinion, and management actions.

Chapter 10 – Expense and Reimbursement Fraud

Case Study: Corporate Card, Digital Invoice and Expense Reimbursement Fraud Risk

Introduction

This case is an anonymized and adapted case study prepared for educational purposes. The company name, period information, amounts, employee titles, vendor names, and transaction details have been rearranged for instructional purposes. Therefore, the case is not intended to directly represent a specific company, but rather to discuss potential fraud , errors, and internal control weaknesses that may arise in expense and cost reimbursement processes.

This case examines expense and reimbursement fraud risks at Orion A.Ş. through its corporate credit card expenditures, personnel expense reimbursement requests, digital invoice documents, representation and hospitality expenses, travel expenses, and approval processes. While the company's expenses appear to be supported by invoices, receipts, card statements, or expense forms, the fundamental audit issue is whether these expenses are genuinely related to company operations, whether the authenticity of the documents has been verified, and whether the approval mechanism is functioning effectively.

The main purpose of this case is to demonstrate that expense auditing is not limited to simply asking "do I have the documentation?". The company purpose of the expenditure, the reliability of the documentation, the integrity of the digital evidence, the risk of duplicate payments, the possibility of personal expenses, the adequacy of the approval process, and the independent control of executive expenses must all be considered together.

This case study aims to have students analyze expense and cost reimbursement processes from the perspectives of corporate card usage, digital invoice manipulation, duplicate expense reimbursements, representation and hospitality expenses, travel expenses, and internal control design. Specifically, risk areas such as recording personal expenses as company expenses, reusing the same document multiple times, altering PDF documents, and expensing canceled trips are discussed.

10.1. Case Background

Orion A.Ş. is a medium-sized service company operating in the fields of tourism, event organization, and corporate services. The company's headquarters are located in Istanbul, and it also has operational offices in Antalya, Bodrum, and İzmir. The company's revenue model consists of income from corporate event services, tourism organizations, yacht and transfer services, accommodation brokerage, and consulting services.

The internal audit conducted on the company's financial statements as of December 31, 2025, specifically examined general administrative expenses, travel expenses , representation and hospitality expenses , corporate card expenditures , personnel expense reimbursements , and digital invoicing processes in detail.

The audit team identified unusual increases in some expense items compared to previous periods. While some of these increases appear to be explainable by growth in business volume, some expenditures were found to be weak in terms of documentation quality, approval process, adequacy of explanation, and commercial justification.

Significant risk concentrations have been identified, particularly in three areas:

1. Using corporate credit cards for personal purposes.
2. Altering or duplicate using digital invoices

3. Insufficient approval and document verification in expense reimbursement requests.

Therefore, the audit has been expanded to include not only the accuracy of accounting records but also internal control weaknesses and potential indicators of fraud in the expense generation process.

10.2. Main Issue of the Case

At Orion A.Ş. is not simply whether expenses are recorded in the accounting records. The real issue is whether these expenses are genuinely related to company operations, whether they are supported by valid and authentic documentation, whether they have undergone proper approval processes, and whether they carry the risk of personal spending, duplicate payments, or digital document manipulation.

Corporate credit card spending, representation and hospitality expenses, travel and accommodation expenses, personnel expense reimbursements, and digital invoicing documents constitute a significant portion of the company's expense structure. While these expense items appear to be documented, they can pose a risk of abuse if the company purpose explanation is weak, the approval process remains formal, or the authenticity of the documents is not verified.

The fundamental control question of the case is this:

At Orion A.Ş., are expense and cost reimbursement processes based on actual, appropriate, documented expenses related to company operations; or are company expenses shown as higher than they actually are or as incorrect due to personal use of corporate cards, alteration of digital invoices, reuse of the same document multiple times, incomplete business purpose explanations, and inadequate approval checks?

To answer this question, the auditor should not only look at whether an invoice, receipt, or card statement is available. The purpose of the expenditure, participant list, customer or project connection, document authenticity, PDF change traces, duplicate document usage,

card statement-expense form consistency, PNR/ticket usage status, and approval authorizations should all be evaluated together.

10.3. Financial Summary, Expenses Structure and Control Scope

Orion A.Ş. reported total general administrative expenses of USD 1,245,000 as of December 31, 2025. The breakdown of these expenses by category and their respective shares in total expenses are presented in Table 10.1.

Table 10.1. General Administrative *Expenses* of Orion A.Ş.

Expense Item	**Amount (USD)**	**Share of the Total**
Staff wages and benefits expenses	412,000	33.1%
Travel and accommodation expenses	186,500	15.0%
Representation and hospitality expenses	142,800	11.5%
Consulting and outsourcing expenses	134,600	10.8%
Corporate credit card spending	118,400	9.5%
Communication and mobile line expenses	49,200	4.0%
Vehicle, fuel and maintenance costs	62,700	5.0%
Office and stationery expenses	28,500	2.3%
Digital subscription and software expenses	38,900	3.1%

Expense Item	**Amount (USD)**	**Share of the Total**
Other various expenses	71,400	5.7%
Total	**1,245,000**	**100%**

During the audit , travel and accommodation expenses , representation and hospitality expenses, corporate card spending , and various other expenses were specifically identified as high-risk areas. These items totaled 519,100 USD , representing approximately 41.7% of total general administrative expenses .

This ratio is important in terms of the risk of expense misuse . This is because such expenses are often difficult to directly link to the company activity, the quality of documentation and explanations varies, they are subject to managerial discretion, and are susceptible to misuse .

The primary objective of this internal audit is to evaluate the accuracy, appropriateness, and effectiveness of internal controls over the expense and cost reimbursement processes at Orion A.Ş. The audit scope and related control areas are summarized in Table 10.2.

Table 10.2. Internal *Audit* Scope for Orion A.Ş.'s Expense and Cost Reimbursement Processes

Area of Control	**Scope of Review**
Corporate credit card spending	Card limits, spending types, personal expense risk, approval processes.
Staff expense reimbursements	Invoice, receipt, travel form, expense description, payment eligibility.
Digital invoicing process	E-invoice/e-archive records, document duplicates, PDF changes

Area of Control	**Scope of Review**
Travel expenses	Airfare, hotel, transfers, domestic/international per diem allowances.
Representation and hospitality expenses	Business objective, invitation list, customer relationship, reasonableness of price
Consulting and outsourcing invoices	Proof of actual service receipt, contract and delivery evidence.
Accounting records	Expense classification, periodic accuracy, account matching.
Authorization and approval checks	Expenditure approval matrices, separation of duties, limit controls.

The specific objectives of the audit are as follows:

- To determine whether personal expenses are recorded as company expenses.
- To test whether the same invoice has been subject to a reimbursement claim multiple times.
- To examine whether any changes have been made to the digital documents.
- To evaluate whether expenditure approvals comply with the authorization matrix.
- To determine if there is a lack of independent control over the management cards.
- Investigating the relationship of expenses to the company activity and their commercial justification.

10.4. High-Risk Process Areas and Control Weaknesses

Orion A.Ş.'s expense and cost reimbursement processes reveals that the risks do not stem solely from individual erroneous expense

records. When corporate card usage, personnel expense reimbursements, digital invoice documents, representation and hospitality expenses, travel expenses, and management approval processes are considered together, it becomes clear that the company has systemic control weaknesses in its expense management process.

Therefore, suspicious transaction areas should be evaluated not only on the basis of "are there documents?", but also in terms of the purpose of the expenditure, the authenticity of the documents, the integrity of the digital evidence, the risk of duplicate payments, the efficiency of the approval process, and the possibility of personal spending.

10.4.1. Corporate Card Misuse Usage Risk

At Orion A.Ş., corporate credit cards have been issued to a total of 18 employees as of 2025. Of these cards, five are used by senior management, seven by sales and operations managers, and six by field operations teams. Although the company has a written corporate card policy, practical implementation appears to be weak. Card statements and supporting expense documents are not systematically reconciled, business purpose explanations are not adequately scrutinized, and certain managerial expenses are not subject to sufficient control.

As shown in Table 10.3, a significant portion of the reviewed corporate credit card spending exhibits weaknesses in terms of business justification, documentation adequacy, approval discipline, and compliance with spending limits. These findings indicate that the company's corporate credit card controls are not sufficiently effective in preventing personal expenses, unsupported transactions, and limit circumvention.

Table 10.3. High-Risk Corporate Credit Card Spending Identified in Orion A.Ş. in 2025

Type of Finding	**Number of Transactions**	**Amount (USD)**
Restaurant expenses with no stated business purpose	26	8,420
Weekend expenses unrelated to business operations	14	5,180
Shopping expenses appearing to be personal in nature	9	4,960
Card charges with missing supporting documentation	18	6,340
Transactions manually approved after exceeding the limit	7	3,850
Suspected split transactions on the same day	6	4,000
Total	**80**	**32,750**

This table shows that a significant portion of card spending exhibits weaknesses in terms of business purpose, document quality, and approval process. In particular, spending on restaurants, accommodation, technology stores, online shopping, spas , and personal consumption should be considered a red flag by the auditor.

The primary risk with corporate card spending is the use of company resources for personal purposes. Expenses such as clothing, personal electronics, weekend stays, spa treatments, or restaurant bills with unclear explanations should be questioned if they cannot be clearly linked to a client, project, field assignment, or company activity.

In this context, corporate card policies should be strengthened; invoices, business purpose explanations, customer/project links, and, where necessary, participant lists should be made mandatory for every transaction. Transactions made on weekends, holidays, high-value transactions, and in sectors carrying a risk of personal spending should automatically be subject to second-level financial approval.

10.4.2. Digital Invoice Manipulation and Duplicate Expense Reimbursement Risk

At Orion A.Ş. , expense documents are largely collected digitally. Personnel upload expense receipts or invoices to the system via a mobile application; after the unit manager approves, the accounting department creates a payment record. While this structure appears fast from an operational perspective, it creates a risk of manipulation and duplicate payments if the integrity of digital documents is not adequately secured.

The following control deficiencies were identified during the audit:

- PDF documents should not be stored in an unchangeable format within the system.
- The absence of an automatic control that prevents the same document from being uploaded again,
- The invoice number, date, amount, and tax identification number fields are not required to be matched using OCR.
- Not actively using the e-invoice/e-archive verification integration,
- Failure to perform checks for abnormal delays between the document upload date and the invoice date,
- Manual approvals are not regularly monitored through system logs

Data analytics procedures conducted on expense reimbursement records identified 47 potential duplicate entries out of a total of 3,842 expense documents. A detailed review showed that 18 of these transactions carried a genuine risk of duplicate payment. These duplicate reimbursement risk indicators are summarized in Table 10.4.

Table 10.4. Duplicate Expense Reimbursement Risks Identified Through Data Analytics

Type of Duplication	**Number of Transactions**	**Amount (USD)**
Two payments with the same invoice number	6	3,420
Same document image uploaded with a different description	5	2,180
Same hotel invoice claimed by two different staff members	3	1,950
Same restaurant receipt uploaded with different dates	4	1,140
Total	**18**	**8,690**

These findings indicate that automatic verification and duplication control in the digital document system are inadequate. Uploading the same invoice with different descriptions, reusing document images, or having different staff members request the same hotel/restaurant document directly creates a risk of financial misuse .

Furthermore, an examination of the PDF metadata and document images in some documents revealed suspicions of amount alteration. For example, a hotel invoice uploaded to the system as 2,450 USD was found to be 1,450 USD in the verification document obtained directly from the hotel, resulting in a discrepancy of 1,000 USD. This is a high-risk finding in terms of digital document manipulation.

Therefore, the expense system should be integrated with e-invoice/e-archive verification platforms, invoice number-vendor-date-amount combinations should be automatically checked, PDF metadata and file hash checks should be applied, and information on the document should be compared with the information entered into the system by personnel using OCR.

10.4.3. Representation , Hospitality And Trip Expenses Risk

Representation, hospitality, and travel expenses are types of expenses where the line between business use and personal use is not always clear. Therefore, the auditor should evaluate these expenses not only in terms of the existence of documentation, but also in terms of client relationship, project connection, participant list, purpose of travel, ticket usage status, and the reasonableness of the expenditure.

The total representation and hospitality expenses at Orion A.Ş. amount to 142,800 USD. Of this amount, 37,600 USD lacks sufficient explanation regarding client name, meeting purpose, participant list, or project affiliation. General descriptions such as "client dinner," "operations meeting," or "supplier meeting" are insufficient to prove the expenditure's connection to business purposes.

Regarding travel expenses, there is a risk that canceled or refunded tickets may be claimed as personnel expenses. Following confirmation with the travel agency, it was determined that two canceled or refunded airline tickets had been recorded as personnel travel expenses. These exceptions are summarized in Table 10.5.

Table 10.5. Canceled or Refunded Airline Tickets Charged as Personnel Travel Expenses

Employee	Ticket Date	Claimed Amount (USD)	Status
Regional Manager C	June 18, 2025	720	Ticket canceled
Sales Specialist D	September 4, 2025	620	Ticket refunded
Total		1,340	

Canceled, refunded, or unused tickets cannot be recorded as company expenses. For travel expenses to be accepted, the trip must have taken place, been for business purposes, and be supported by valid documentation. Therefore, PNR and usage status checks should be

mandatory for airline tickets, integration should be established between travel agencies and the expense system, and cancellation/refund reports should be regularly submitted to the accounting department.

10.4.4. Systemic And Behavioral Red Flags

The audit identified several red flags that may indicate expense and cost reimbursement fraud. These indicators alone do not constitute definitive evidence of fraud; however, when considered together, they suggest a significant control risk in the expense management process. The main behavioral and operational red flags are summarized in Table 10.6.

Table 10.6. Behavioral and Operational Red Flags in Orion A.Ş.'s Expense and Cost Reimbursement Process

Red Flag	**Explanation**
Document descriptions are general and vague	Inadequate explanations such as "customer meeting," "operating expense," and "project cost"
Spending tends to concentrate at the end of the month	Possible budget use pressure or attempts to exhaust remaining limits
High-volume transactions occur on weekends and holidays	Risk of personal spending
Frequent small purchases are made from the same vendors	Risk of transaction splitting or approval limit circumvention
Documents are uploaded long after the expenditure date	Risk of document manipulation or subsequent editing
Executive expenses are subject to limited scrutiny	Risk of senior management override or exception-based approval
The same invoice is uploaded with different descriptions	Risk of duplicate reimbursement or manipulation
There are discrepancies between card statements and expense forms	Risk of incomplete or inaccurate accounting

Financial red flags are also noteworthy. In this context, the 48% increase in travel expenses compared to the previous year, the 62% increase in representation and hospitality expenses, incomplete explanations in 28% of corporate card spending, late document uploads in 12% of expense reimbursements, duplicate payment risk amounting to USD 8,690, and suspected personal spending amounting to USD 4,960 should be considered together.

These indicators reinforce the need for stronger approval controls, automated document matching, and continuous monitoring of expense transactions. These indicators show that the risk in the expense and cost reimbursement process stems not only from individual behavior but also from control design, lack of systemic verification, and weak approval mechanisms.

10.4.5. Internal Control vulnerabilities

The control deficiencies identified in the expense and cost reimbursement process at Orion A.Ş. can be evaluated in three main groups: deficiencies in control design, deficiencies in control implementation, and deficiencies in monitoring.

From a control design perspective, the spending policy contains general statements; prohibited spending types, documentation requirements, and the evidence required for representation expenses are not sufficiently clearly defined. The absence of an independent control mechanism for executive expenses and the lack of systemic matching between corporate card spending and expense forms are significant design deficiencies.

From a control perspective, it appears that approving managers do not adequately question the company purpose of the expenditure, the accounting unit mostly focuses on document existence, and examines document content and business rationale only to a limited extent. The fact that transactions exceeding limits can be approved manually and that late-uploaded documents are not marked as risky transactions by the system also weakens the effectiveness of control.

In terms of monitoring, the main shortcomings are the failure to prepare monthly exception reports for cardholders, the lack of separate monitoring of weekend and holiday transactions, the absence of merchant-based spending concentration analyses, and the inconsistent review of audit trail records.

Overall, the main control problem in Orion A.Ş.'s expense and cost reimbursement process is that, despite the documents being uploaded to the system, their authenticity, relevance to the company purpose, and whether they are being used duplicated are not sufficiently verified. Therefore, the control structure should be based not only on manual approval but also on systemic blocking, automated verification, data analytics, and independent financial control mechanisms.

10.5. Potential Expense Reimbursement Fraud Scenario

The findings in the Orion A.Ş. case do not, by themselves, mean that every single expense was fraudulent. However, when corporate card expenditures, digital invoice documents, representation and hospitality expenses, travel expenses, and manual approval processes are considered together, it is evident that there is a systematic control weakness in the expense and expense reimbursement process.

In a possible scenario, some employees or managers may have used corporate credit cards for expenses not directly related to company operations. Purchases such as restaurants, weekend stays, personal shopping, spa treatments, or electronics pose a personal spending risk if adequate business purpose explanation and supporting documentation are lacking. Such transactions can lead to company expenses being overstated and company resources being used for personal purposes.

The digital invoicing process is also a crucial part of this scenario. Uploading expense documents to the system via a mobile application has provided operational convenience; however, automatic e-invoice verification, OCR matching, PDF metadata control, and duplicate document prevention controls are not sufficiently robust. Therefore, there is a risk of the same document being reused with different descriptions, amounts

being altered on the PDF, or the same invoice being subject to expense refunds multiple times.

Inadequate business purpose descriptions for representation and hospitality expenses obscure the commercial nature of the expenditure. Generic terms such as "client dinner," "operations meeting," or "supplier meeting" should not be considered sufficient for audit evidence unless supported by client name, participant list, meeting purpose, and project affiliation. This increases the risk of personal consumption being presented as representation expenses.

In travel expenses, claiming canceled or refunded tickets as expenses can result in uncompleted trips becoming company expenses. Without automatic integration between travel agency records and the expense system, erroneous or unjustified expense refunds based on employee declarations may not be detected in a timely manner.

In this scenario, the fact that management approvals remain purely formal is also a significant risk factor. Approving expenditures solely based on the existence of documentation is insufficient to verify the expenditure's relevance to the company purpose, the authenticity of the documentation, and the reasonableness of the amount. In particular, the lack of independent financial audits of senior management and director cards weakens the control environment.

Based on the audit findings, the risk assessment regarding Orion A.Ş.'s expense and cost reimbursement process can be summarized in Table 10.7.

Table 10.7. Risk Assessment of Orion A.Ş.'s Expense and Cost Reimbursement Process

Risk Area	**Likelihood**	**Impact**	**Risk Level**
Personal use of corporate cards	High	Medium	High
Digital invoice manipulation	Medium	High	High

Duplicate expense reimbursement	Medium	Medium	Medium-High
Misuse of representation expenses	High	Medium	High
Payment of canceled/refunded travel expenses	Medium	Medium	Medium
Managerial approvals remaining merely formal	High	High	Very High
Payments with missing supporting documents	Medium	Medium	Medium
Fake vendor or related-party invoices	Low-Medium	High	Medium-High

This risk assessment indicates that the expense and cost reimbursement process at Orion A.Ş. is a high-risk area. The root cause of the risk is not solely individual inappropriate transactions. The main problem stems from insufficient transparency in spending policies, weak digital document verification controls, reliance on manual review for duplicate payment controls, lack of independent auditing of executive expenses, and the absence of regular data analytics monitoring of risky transactions.

This structure doesn't directly mean all expenses are fraudulent. However, when considering factors such as suspicion of personal spending, risk of duplicate payments, PDF document alterations, incomplete business purpose descriptions, expense claims for canceled tickets, and ineffective management approvals, it's clear that the company faces a significant risk of misuse in its expense control process .

Therefore, the auditor's primary priority is not simply to check whether expenses have been recorded. The auditor should evaluate the veracity of the expenditure, its relevance to the company purpose, the authenticity of the document, the likelihood of duplicate use, the results of third-party verification, and the effectiveness of the approval process. Based on this evaluation, actions such as recourse against personnel, correction entries, disciplinary proceedings, and

control improvement actions should be considered for inappropriate expenditures.

10.6. Audit Procedures , Data Analytics And Control Evaluation

Orion A.Ş.'s expense and cost reimbursement should not be limited solely to invoice, receipt, or card statement checks. The authenticity of the expenditure, its relevance to the company purpose, the originality of the document, whether it was used repeatedly, the effectiveness of the approval process, and the adequacy of systemic controls should all be evaluated together. Therefore, audit procedures should be designed to include document review, data analytics, third-party verification, and internal control assessment.

10.6.1. Document Examination Procedures

The auditor should first review documents related to corporate card charges, employee expense reimbursements, representation and hospitality expenses, travel expenses, and digital invoices. This includes comparing invoice dates with payment dates, matching card statements with expense forms, verifying the adequacy of expense descriptions, and evaluating the connection of each expense to a customer, project, meeting, or operational activity.

Table 10.8. Document Review Procedures for Orion A.Ş.'s Expense and Cost Reimbursement Audit

Procedure	Aim
Comparing invoice date and payment date.	Identifying the risk of delayed or subsequently generated documents.
Invoice number retest	Identifying the risk of duplicate payments.
Seller name and IBAN match	Examining the risk of counterfeit or affiliated vendors.
PDF metadata analysis	Analyzing suspicions of digital document alteration.

Reconciliation of credit card statement and expense form.	To test whether card spending has been accurately reported.
Expense statement adequacy check	To evaluate the company purpose and commercial rationale.
Administrator approval trail check	Testing compliance with the authorization matrix.

As shown in Table 10.8, document review procedures should not be limited to checking the existence of invoices or receipts. The auditor should also evaluate timing, consistency, business rationale, approval evidence, and the possibility of digital manipulation in order to assess the reliability of expense transactions.

10.6.2. Data Analytics Procedures

Expense and corporate card data contain too many transactions to be fully reviewed manually. Therefore, the auditor should use data analytics procedures in the expense reimbursement process. The main analytical tests and their audit purposes are summarized in Table 10.9.

Table 10.9. Data Analytics Procedures for Orion A.Ş.'s Expense and Corporate Card Transactions

Analytical Test	**Audit Purpose**
Same amount, same vendor, and close-date test	To identify potential duplicate payments
Weekend spending analysis	To identify expenses with weak business justification or potential personal use
Below-limit split transaction analysis	To detect transactions split to avoid approval limits
Round-amount spending test	To identify artificial or unusual spending patterns
Card-user-based anomaly analysis	To identify employees with unusual spending behavior
Vendor concentration analysis	To detect unusual spending accumulation at specific vendors
Late document upload analysis	To assess the risk of subsequently edited, altered, or generated documents

These tests should be used to identify high-risk users, vendors, expense types, and periods. Detailed sample selection should then be based on the risk indicators generated through these analytical procedures.

10.6.3. Third-Party Verification Procedures

For certain high-risk expenses, the auditor should not rely solely on documentation provided by employees. Third-party verification should be obtained, particularly for hotel invoices, airline tickets, restaurant charges, technology purchases, and consulting invoices. The relevant verification procedures and audit purposes are summarized in Table 10.10.

Table 10.10. Third-Party Verification Procedures for High-Risk Expense Transactions

Type of Spending	Verification Source	Audit Purpose
Hotel invoices	Hotel accounting department	To verify the accuracy of the invoice amount and accommodation details
Airline tickets	Travel agency or airline records	To verify whether the ticket was used, canceled, or refunded
Restaurant expenses	Vendor POS or reservation records	To verify the number of attendees and the business purpose of the expense
Technology purchases	Company inventory records	To determine whether the purchased item was recorded as a company asset
Consulting invoices	Service reports and delivery evidence	To evaluate whether the service was actually received

These procedures are particularly important for identifying risks such as document manipulation, cancelled or refunded travel expenses, personal spending, and payments for services not actually received.

10.6.4. Internal Control Evaluation

The audit should also evaluate Orion A.Ş.'s internal control structure over the expense and cost reimbursement process. The current findings indicate that control weaknesses stem not only from individual errors, but also from deficiencies in control design and operating effectiveness. The main control vulnerabilities are summarized in Table 10.11.

Table 10.11. Control Vulnerabilities in Orion A.Ş.'s Expense and Cost Reimbursement Process

Control Area	Current Weakness	Risk
Spending policy	The policy contains general and ambiguous statements	Risk of inconsistent interpretation by employees
Document requirements	Required documents are not standardized by expense type	Risk of payments being made with missing or insufficient documentation
Executive expenses	Independent financial oversight is weak	Risk of senior management override or exception-based approval
Representation expenses	Participant lists are not mandatory	Uncertainty regarding the business purpose of expenses
Corporate cards	Card statements and expense forms are not automatically matched	Risk of inaccurate or incomplete expense declarations
Digital invoices	E-invoice verification and PDF integrity checks are weak	Risk of forged or altered documents
Monitoring activities	Monthly exception reports are not prepared regularly	Risk of delayed detection of high-risk transactions

Therefore, the audit assessment should focus not only on the existence of supporting documentation, but also on the design of internal controls, their operating effectiveness, and the adequacy of monitoring mechanisms.

10.6.5. Recommended Control Matrix

To reduce expense and cost reimbursement risks at Orion A.Ş., the following control matrix should be implemented. The matrix links each identified risk to a recommended control activity, control type, and responsible unit, as summarized in Table 10.12.

Table 10.12. Recommended Control Matrix for Orion A.Ş.'s Expense and Cost Reimbursement Risks

Risk	Recommended Control	Control Type	Responsible Unit
Personal expenses are made using corporate cards	Prohibited spending categories and automatic MCC blocking	Preventive	Finance / IT
Payments are made with missing documents	Payment approval screen cannot proceed before document upload	Preventive	Accounting
Duplicate invoice usage	Automatic matching based on invoice number, vendor, date, and amount	Preventive	IT / Accounting
PDF document manipulation	File hash and metadata checks	Detective	IT / Internal Audit
Misuse of representation expenses	Mandatory participant list and business purpose requirement	Preventive	Sales / Finance
Canceled or refunded tickets are claimed as expenses	PNR usage and refund status verification	Detective	Accounting
Managerial approvals are ineffective	Second-level financial approval for risky transactions	Preventive	Finance Directorate
Weekend and holiday spending risk	Automatic exception reports for weekend and holiday transactions	Detective	Internal Audit
Transaction splitting below approval limits	Same-day, same-vendor, and same-user split transaction analysis	Detective	Internal Audit
Anomalies in spending trends	Monthly analytics dashboard	Monitoring	Financial Planning / Internal Audit

This control matrix aims to prevent inappropriate spending before transactions are processed and to identify risky transactions promptly

after they occur. Accordingly, preventive controls should be embedded into the ERP and payment approval workflow, while detective and monitoring controls should support regular internal audit review.

10.6.6. Management Action Plan

To prevent the recurrence of the audit findings, Orion A.Ş. management should develop a short- and medium-term action plan. The recommended corrective actions, priorities, responsible units, and target completion periods are summarized in Table 10.13.

Table 10.13. Management Action Plan for Preventing Recurrence of Expense and Cost Reimbursement Findings

Action	**Priority**	**Responsible Unit**	**Target Completion Period**
Update the corporate card policy	High	Finance Director	30 days
Add duplicate invoice checks to the expense system	High	IT / Accounting	60 days
Activate e-invoice verification integration	High	IT	90 days
Revise the representation expense form	Medium	Sales / Finance	45 days
Establish an independent approval mechanism for executive expenses	High	General Directorate	30 days
Prepare monthly exception reports for risky transactions	Medium	Internal Audit	30 days
Recover personal expenses charged to the company from responsible employees	High	Human Resources / Finance	15 days
Provide training on expense reimbursement procedures	Medium	Human Resources	60 days
Implement a cancellation/refund ticket verification report	Medium	Accounting	45 days

This action plan aims not only to correct previously identified irregular practices, but also to prevent similar expense and reimbursement risks from recurring in the future.

10.6.7. General Evaluation

Overall, the primary purpose of expense and cost reimbursement audits at Orion A.Ş. is not merely to verify the existence of documents. The auditor should analyze each expense's relevance to the company purpose, the authenticity of the documents, the likelihood of duplicate use, the effectiveness of the approval process, and whether it is supported by systemic controls.

In this context, preventive, detective, and monitoring controls must work together in the expense management process. Otherwise, corporate card usage, digital invoice uploading, representation expenses, and travel expenses can create financial losses, ethical vulnerabilities, tax risks, and internal control reliability problems for the company.

10.7. Findings, Auditor's Assessment and Recommendations

Orion A.Ş.'s corporate card, expense reimbursement, representation-hospitality, and travel expenses reveals significant risk areas such as the misuse of company resources for personal purposes, manipulation of digital invoice documents, duplicate expense reimbursements, and the expense recognition of canceled travel documents . The findings indicate weaknesses in the expense management process regarding document verification, business purpose control, digital document reliability, independent review of executive expenses, and systemic preventative controls.

Table 10.14. Summary of Key Audit Findings in Orion A.Ş.'s Expense and Cost Reimbursement Process

	Finding	**Auditor's Assessment**	**Suggestion**
1	Personal use is suspected in corporate card transactions. A total of 4,960 USD in corporate credit card spending was identified as suspicious for personal use. These expenses included clothing, personal electronics, spa services, and weekend accommodations.	According to the company's spending policy, corporate cards should only be used for expenses directly related to company operations. Expenses identified that are not linked to business purposes pose a risk of company assets being used for personal purposes. This can lead to expenses being overstated, the risk of expenses not being legally deductible from tax records, weakening management control, and damaging ethical culture. In particular, the lack of independent control over executive and manager expenses represents a significant weakness in the control environment.	Expenses deemed personal should be recouped from the employee. The corporate card policy should be republished and signed by the employee. Business purpose, participant list, and documentation should be mandatory for every card transaction. Weekend and holiday expenses should automatically be subject to second-level approval. Executive cards should also be subject to independent financial audits.
2	There is a risk of digital invoice manipulation and duplicate expense refunds. Analysis of documents uploaded to the expense system revealed a risk of duplicate payments amounting to 8,690 USD and suspicion of PDF document alterations amounting to 1,000 USD.	Expense reimbursements must be based solely on genuine, valid, original documents related to the company's activities. Using the same document for multiple payment requests or altering a PDF document directly creates a risk of financial loss and expense recording based on fraudulent documents. The lack of e-	The expense system should be integrated with e-invoice/e-archive verification platforms. The system should automatically prevent duplicate invoice number, vendor, date, and amount combinations. PDF metadata and file hash verification should be implemented. Expense documents should be read using OCR and

		invoice verification integration, the absence of system controls preventing duplicate invoice numbers, and accounting control based solely on document images further exacerbate this risk.	automatically compared with the entered information. Amounts found to be duplicated should be recovered, and disciplinary action should be taken against the relevant personnel.
3	The documentation for the purpose of the company is insufficient in the representation and hospitality expenses. The total representation and hospitality expenses amount to 142,800 USD. Of this amount, 37,600 USD lacks adequate explanation regarding client name, meeting purpose, participant list, or project affiliation.	Representation and hospitality expenses must be clearly related to business activity and supported by customer, supplier, project, or business development objectives. Expenses not documented as business-related increase the risk of personal consumption being recorded as company expenses. Furthermore, such expenses may be subject to tax rejection, lead to inaccurate expense budgeting, and distort the expenditure structure in management reports. The shift of management approval from content control to formal approval weakens the effectiveness of control.	A participant list, company name, and meeting purpose should be mandatory for representation expenses. Second-level approval should be required for representation expenses exceeding 500 USD. Expenses unrelated to a client or project should not be eligible for reimbursement. Representation expenses should be analyzed monthly by individual, vendor, client, and project.
4	Canceled tickets were expensed in travel costs. Following verification by the travel agency, it was determined that two cancelled or refunded airline tickets were	Canceled, refunded, or unused tickets cannot be recorded as company expenses. For travel expenses to be deductible , the trip must have taken place, been for business purposes, and be	PNR and usage status checks should be made mandatory for airline tickets. Travel agencies should submit monthly cancellation/refund reports to the accounting department. Automatic

	included in personnel expenses. The total amount is 1,340 USD . It was determined that a ticket belonging to Regional Manager C, dated June 18, 2025, for 720 USD, was cancelled; and a ticket belonging to Sales Specialist D, dated September 4, 2025, for 620 USD, was refunded.	supported by valid documentation. The lack of integration between travel agency records and the expense system has led to the deduction of unused tickets as expenses and unjustified expense reimbursements. This situation points to inaccurate tracking of the travel budget and a risk of misuse by personnel .	blocking of refunded or canceled tickets should be implemented in the expense system. Incorrectly paid amounts should be recovered from the relevant personnel, and integration should be established between the travel system and the expense system to prevent recurrence.

Overall, the primary risk in Orion A.Ş.'s expense and expenditure management process is not whether expenses are recorded, but rather whether these expenses are directly related to business purposes, supported by valid and authentic documentation, and verified through systemic controls. When corporate card expenses, representation and hospitality expenses, digital invoice documents, and travel expenses are considered together, it is evident that the company has significant control deficiencies in its expense management process, both in terms of ethics and financial reporting.

This structure alone does not indicate that all expenses are fraudulent. However, when personal expense suspicion, the risk of duplicate payments, PDF document alterations, representation expenses with incomplete business purpose descriptions, and the reimbursement of canceled tickets are considered together, it is clear that a high-risk area has emerged in the company's expense control process. For the auditor, the primary priority is to test the authenticity of expenses, their relevance to business purposes, the authenticity of documents, the repetition of payments, and the effectiveness of approval processes.

10.8. Instructor Notes

This case is designed to allow students to evaluate the expense and cost reimbursement process not only on the basis of "do you have documentation?", but also in terms of the purpose of the expenditure, the authenticity of the documentation, the approval process, the integrity of digital evidence, and ethical risks. In the case of Orion A.Ş., some expenses appear to be supported by invoices, card statements, or expense forms; however, the main audit risk is whether these expenses are truly related to the company's business activities.

Students should be expected to discuss issues such as the use of corporate cards for personal purposes, the alteration of digital invoices, the use of the same document for multiple expense claims, insufficient explanation of business purpose in representation and hospitality expenses, and the expenseing of canceled travel tickets .

This case demonstrates that expense fraud doesn't always involve large-scale transactions. Small, recurring personal expenses, incomplete disclosures, duplicate documents, PDF alterations, and poor approval processes, when combined, can lead to significant financial loss, tax risk, and ethical vulnerabilities.

During the learning process, students should be expected to evaluate each finding from three perspectives: the nature of the expenditure, its financial/ethical impact, and the recommended control measures that should be implemented. Therefore, students should not be satisfied with simply stating "invoice exists" or "manager approved"; they should question the relationship of the expenditure to the company purpose, the reliability of the document, and the effectiveness of the control process.

In conclusion, the Orion A.Ş. case demonstrates the importance of professional skepticism in expense auditing. The auditor should assess not merely whether the expense was recorded, but whether it is genuine, appropriate, documented, authentic, and related to the company's operations.

10.9. Discussion Questions

1. What are the three most significant risks in the expense and cost reimbursement process at Orion A.Ş. ?
2. What indicators can be used to understand the risk of personal use in corporate card spending?
3. Why do expenditures with missing documentation or insufficient explanations create an audit risk?
4. How should the purpose of business be documented for representation and hospitality expenses?
5. Why is it risky to not subject executive expenses to independent control?
6. In what situations are weekend and holiday credit card purchases considered a red flag?
7. Uploading the same invoice to the system with different descriptions indicates what type of fraud risk?
8. Why are PDF metadata checks and e-invoice verification important in expense auditing?
9. What financial and ethical risks arise from recording canceled or refunded tickets as expenses?
10. What control purpose do MCC blocking and second-level authentication serve in corporate card transactions?
11. What are the three most urgent control recommendations that need to be implemented for Orion A.Ş.?
12. How does this case illustrate the difference between "document existence" and "document reliability" in expense auditing?

10.10. Conclusion

Orion A.Ş.'s expense and cost reimbursement processes as of December 31, 2025, reveals significant control deficiencies in the company's expense management. Specifically, systematic shortcomings exist in areas such as corporate card usage, digital invoice verification, duplicate expense control, and documentation of representation and hospitality expenses.

The audit revealed a total of 32,750 USD in high-risk corporate card spending, 8,690 USD in duplicate payment risk, 4,960 USD in suspected personal spending, and 1,000 USD in suspected digital invoice manipulation.

These findings should not be interpreted as direct, definitive fraud ; however, they indicate that the company's current control environment is vulnerable to expense fraud . In the short term, Orion A.Ş. needs to update its corporate card policy, strengthen digital invoice verification controls, implement automated duplication tests on its expense system, and subject executive expenses to independent auditing.

As a general audit opinion, it has been concluded that the expense and cost reimbursement process at Orion A.Ş., in its current form, is high-risk , but that the risk level can be reduced to a reasonable level if the proposed controls are implemented.

Appendix 10.1. Audit Questionnaire

Orion A.Ş. Expense and Reimbursement Fraud Questionnaire

	Area of Control	**Question**	**Objective / Audit Risk**
1	Pricing Policy	Does the company have a written corporate card and refund policy?	To assess whether the expense process is based on written rules.
2	Policy Approval	Has the expense policy been communicated to and signed by all staff?	To reduce the risk of allegations that staff are unaware of the rules and to minimize inconsistencies in application.
3	Corporate Card Usage	Are corporate cards only used for expenses directly related to company operations?	Testing the risk of recording personal expenses as company expenses.
4	Personal Spending Risk	Are clothing, personal electronics, spa treatments, and vacation or weekend stays reported separately?	To identify personal expenses.
5	Card Spending Receipt	Is there an invoice, receipt, or valid document for each card transaction?	Reducing the risk of recording expenses without documentation.
6	Business Purpose Statement	Is the purpose of the company clearly and adequately stated in each expense request?	Assessing the risk of classifying non-business expenses as business expenses.

	Area of Control	**Question**	**Objective / Audit Risk**
7	Participant List	Do the participant list and company information appear in the representation and hospitality expense records?	To test the connection between representation expenses and business activity.
8	Client/Project Connection	Are representation and hospitality expenses associated with a client, supplier, project, or sales opportunity?	Identifying expenses that lack proper documentation for the company purpose.
9	High Amount Approval	Are representation and hospitality expenses exceeding 500 USD subject to second-level approval?	To prevent high-value expenses from being approved through formal processes.
10	Executive Expenses	Are executive and manager card expenditures subject to independent financial audits?	To prevent weaknesses in control over senior staff spending.
11	Weekend Spending	Have expenses incurred on weekends and public holidays been examined separately?	Identify transactions with a weak business purpose or those that may be considered personal expenses.
12	MCC Blockage	Is MCC blocking applied to sector codes that carry a risk of personal spending on corporate cards?	To prevent inappropriate charges at the time of the transaction.

	Area of Control	**Question**	**Objective / Audit Risk**
13	Card Statement Matching	Are the card statement, expense form, and document automatically matched?	To reduce the risk of incorrect expense acceptance due to manual and superficial inspection.
14	Exceeding the limit	Are card limits monitored systematically, and is exceeding the limit subject to a second approval?	To prevent uncontrolled spending by exceeding limits.
15	Reimbursement of Personal Expenses	Are expenses deemed to be personal funds recouped from the employee?	To recover losses resulting from the use of company resources for personal purposes.
16	E-Invoice Verification	Is the expense system integrated with e-invoice or e-archive verification platforms?	To prevent expense reimbursements based on forged or invalid documents.
17	Duplicate Invoice Check	Are the same invoice number, vendor, date, and amount combinations being blocked by the system?	To prevent the same document from being used in multiple expense claims.
18	Similar Document Verification	Are documents uploaded with different descriptions but bearing the same vendor, date, and amount being analyzed?	Identifying the risk of duplicate expense reimbursements.

	Area of Control	**Question**	**Objective / Audit Risk**
19	PDF Metadata Checking	Are the metadata and change history of PDF documents uploaded to the expense system checked?	To enable the detection of altered digital documents.
20	File Hash Check	Is file hash verification performed on uploaded documents ?	To reduce the risk of re-uploading the same or modified file.
21	OCR Control	Are expense documents read using OCR and compared with the information entered by staff?	Identifying the risk of manual data entry errors or intentional data alterations.
22	Seller Verification	Are the vendor details included in the expense documents regularly verified?	To identify counterfeit documents or documents obtained from unregistered vendors.
23	Digital Document Integrity	Are there any controls in place to prevent or detect alterations to digital documents?	Reducing the risk of digital invoicing manipulation.
24	Duplicate Payment Refund	Have the identified duplicate payment amounts been recovered from the relevant personnel?	To ensure direct financial compensation for losses.
25	Disciplinary Process	Has disciplinary action been initiated against personnel who	To prevent abusive behavior and strengthen an ethical culture.

	Area of Control	**Question**	**Objective / Audit Risk**
		submitted forged, altered, or duplicate documents?	
26	Travel Request	Are travel expenses based on a pre-approved travel request?	Preventing non-business travel expenses.
27	PNR Check	Is PNR and usage status checked for airline tickets?	canceled or unused tickets from being expensed .
28	Cancellation/Refund Report	Does the travel agency send a monthly cancellation and refund report to accounting?	To ensure that returned tickets are identified in the expense system.
29	Travel System Integration	Are the travel agency records and expense system integrated?	To reduce erroneous or unjustified expense reimbursements based on employee declarations.
30	Unused Tickets	Is there an automatic payment block for unused, cancelled, or refunded tickets?	To avoid the risk of expense for trips that never took place.
31	Expense Approval Process	Are expense requests reviewed separately by the relevant department manager and the finance department?	To reduce the risk of accepting incorrect expenses through formal approval.
32	Separation of Duties	Are the people who incur the expense, approve it, account for it, and pay it all different?	To prevent errors or misconduct from being committed and concealed by a single individual.

	Area of Control	Question	Objective / Audit Risk
33	Budget Control	Are expenses compared to the budget on a departmental and individual basis?	Identifying unusual increases in expenses.
34	Vendor-Based Analysis	Are expenses and representation costs analyzed on a vendor-by-vendor basis?	Identifying spending patterns that are concentrated at specific vendors or that are suspicious.
35	Personnel-Based Analysis	Are expense requests analyzed by employee based on amount, frequency, and type of expense?	Identifying unusual spending habits.
36	Round Amounts	Are round, recurring, or poorly explained expenses also investigated?	Identifying transactions that carry the risk of artificial or unrealistic expenses.
37	Continuous Monitoring	Has a continuous monitoring panel been established for corporate card, representation, travel, and expense reimbursement transactions?	To ensure that risky expenditures are identified in a timely manner, not at the end of the period.
38	Management Reporting	Are suspicions of personal spending, duplicate payments, missing documents, and high representation expenses regularly reported to management?	To enable management to monitor cost risks.
39	Tax Risk	Are expenses that may be considered legally non-	To reduce the risk of expense rejection and penalties during tax audits.

	Area of Control	**Question**	**Objective / Audit Risk**
		deductible classified separately?	
40	Results Evaluation	Have any significant control lapses, personal use, duplicate payments, or digital document manipulation been identified in the expense process?	To identify the findings and necessary actions to be included in the audit report.

Chapter 11 – Executive-Level Financial Reporting Manipulation

Case Study: Management Override, Reporting Bias and Ethical Implications

Introduction

This case is an anonymized and adapted case study prepared for educational purposes. The company name, period information, amounts, transaction details, and financial statement items have been rearranged for instructional purposes. Therefore, the case is designed to discuss financial statement manipulation, management override, ethical reporting risks, and internal control weaknesses at the senior management level, rather than directly representing a specific company.

This case examines the audit risks arising from Kazey A.Ş. 's financial statements as of December 31, 2025, with respect to financing expenses, depreciation and amortization calculations, debt classification, capital expenditures, discount applications, and related-party transactions. While the company's reported financial statements appear to be based on accounting records, the fundamental audit issue is whether these records accurately reflect the company's true financial position, debt level, net loss, and reporting risks.

The primary purpose of this case is to demonstrate that financial statement manipulation is not limited to falsifying documents or directly inflating revenues. Underreporting expenses, underestimating depreciation and amortization expenses, presenting short-term liabilities as long-term, capitalizing investment expenditures without sufficient documentation, and under-disclosure of related-party transactions are also significant risk areas that can mislead users of financial statements.

This case study aims to have students evaluate the financial reporting process not only from the perspective of technical accounting records, but also in terms of management override, professional skepticism, ethical responsibility, audit committee oversight, and the independence of the internal control system. Specifically, it explores how pressure from senior management to present more favorable financial results can influence accounting estimates, classification decisions, and disclosure levels.

11.1. Case Background

Kazey A.Ş. is a medium-to-large scale service company operating in marina management, tourism facility management, leasing activities, technical services, and fuel sales revenue. The company's business model consists of marina mooring services, marina commercial space rentals, technical services, electricity and water service revenues, fuel sales, and various ancillary business revenues.

Kazey A.Ş.'s primary revenue sources for 2025 consist of marina mooring revenues, rental income, technical service revenues, fuel sales revenue, electricity and water utility revenues, and other ancillary income. These revenue sources are summarized in Table 11.1.

Table 11.1. Primary Revenue Sources of Kazey A.Ş. for 2025

Income Item	**Explanation**
Marina mooring revenues	Annual and seasonal mooring fees collected from boat owners
Rental income	Rental fees from shops, restaurants, and commercial spaces within the marina
Technical service revenues	Revenues from towing, hauling, maintenance, washing, and minor repair services
Fuel sales revenue	Revenues from diesel and gasoline sales
Electricity and water utility revenues	Revenues generated from utility services provided to marina customers
Other income	Commissions, penalties, service fees, and ancillary activity revenues

Throughout 2025, the company made significant investment expenditures to improve marina infrastructure, commercial areas, electrical systems, security systems, pier renovations, and technical service capacity. While these investments aim to increase the company's operational capacity, they have also increased the weight of significant account items on the financial statements, such as fixed assets, rights-of-use assets, special costs, long-term liabilities, and financing expenses.

Kazey A.Ş.'s operating model requires high fixed investment. Therefore, the company's financial performance is closely related not only to operating income but also to the correct capitalization of investment expenditures, accurate calculation of depreciation and amortization expenses, full recording of financing expenses, and the correct classification of liabilities with appropriate maturities.

An internal audit of the financial statements as of December 31, 2025, has raised significant doubts regarding the accuracy of the company's reported financial position. Specifically, key risk areas identified include underreporting of financing expenses, underestimation of depreciation and amortization expenses, presentation of short-term liabilities as long-term, capitalization of investment expenditures without adequate approval and contract revisions, and insufficient transparency in the disclosure of related-party transactions.

The company's investments for 2025 aim to increase its operational capacity. However, the lack of sufficient documentation, board approval, technical acceptance reports, or contract revisions for some investment expenditures suggests that senior management may have bypassed the expenditure approval processes and manipulated the financial statements.

This case examines the possibility that the company's senior management may have presented a more favorable financial outlook for the company through accounting decisions that directly or indirectly affected the financial statements. Therefore, the case should be evaluated not only in terms of technical accounting errors, but also in terms of management override, ethical breaches, financial reporting reliability, audit committee oversight, and internal control deficiencies.

11.2. Main Issue of the Case

In the case of Kazey A.Ş. , the fundamental audit issue is not simply whether the amounts in the financial statements correspond to accounting records. The real issue is assessing whether senior management has influenced accounting estimates, classification decisions, expense records, capital expenditures, and related-party transactions to present a more favorable financial outlook for the company.

The company's financial statements as of December 31, 2025, show a high amount of fixed assets, long-term liabilities, financing expenses, and a net loss for the period. This structure may create pressure on management to present more positive financial results. In particular, the underreporting of financing expenses, the low allocation of depreciation and amortization expenses, the presentation of short-term liabilities as long-term, and the capitalization of some investment expenditures without sufficient approval raise significant doubts about whether the financial statements are presented fairly.

The fundamental control question of the case is this:

Kazey A.Ş.'s financial statements accurately reflect the company's true financial position, debt level, investment costs, and net loss for the period; or have the financial statements become misleading due to senior management's attempts to present a more positive financial performance by underreporting expenses, misclassifying liabilities, overstating assets, and failing to disclose certain transactions with sufficient transparency?

To answer this question, the auditor cannot rely solely on accounting records and management statements. Financing expenses must be recalculated, depreciation and amortization records must be reviewed, the maturity classification of liabilities must be checked, contractual and board approvals for investment expenditures must be examined, related party transactions must be analyzed in detail, and an assessment must be made of whether senior management has exceeded internal control processes.

Therefore, the case should be examined not only in terms of technical accounting errors but also in terms of management override, financial

reporting ethics, audit committee oversight, and the independence of the internal control system.

11.3. Financial Summary, Adjustment Effects, and Control Scope

The review of Kazey A.Ş.'s financial statements as of December 31, 2025, indicates that the company has a substantial fixed asset base, a significant level of long-term debt, and high financing expenses. Although the company generates revenue from its core operations, the effects of financing expenses and capital expenditures on the financial statements are considerable. The company's summary financial outlook as of December 31, 2025, is presented in Table 11.2.

Table 11.2. Summary Financial Outlook of Kazey A.Ş. as of December 31, 2025

Financial Indicator	Amount (USD)
Total assets	27,475,000
Current assets	1,145,000
Fixed assets	26,330,000
Short-term liabilities	191,000
Long-term liabilities	26,790,000
Equity	494,000
Net sales	2,188,000
Gross profit from sales	964,000
Financing expenses	3,382,000
Reported net loss for the period	2,635,000

This table shows that the company is able to generate limited profit from its core operations; however, it reports significant losses due to high financing costs. Furthermore, the weight of fixed assets within total assets and the high level of long-term liabilities indicate that the company's financial situation is closely related to its investment expenditures, debt structure, and financing costs.

During the internal audit, it was determined that certain expenses had been understated and certain liabilities had been misclassified. Following the audit adjustments, the company's net loss is expected to change as summarized in Table 11.3.

Table 11.3. Effect of Audit Adjustments on Kazey A.Ş.'s Net Loss for the Period

Explanation	Impact on Net Loss (USD)
Reported net loss for the period	(2,635,000)
Understated amortization expense	(56,000)
Understated depreciation expense	(72,000)
Unrecorded interest and exchange rate difference expense	(173,000)
Adjusted net loss for the period	(2,936,000)

The audit adjustments presented in Table 11.3 show that Kazey A.Ş.'s net loss should have been approximately USD 301,000 higher than initially reported, increasing from USD 2,635,000 to USD 2,936,000. This discrepancy should not be considered merely a technical accounting error. The understatement of financing expenses, depreciation and amortization expenses, and the misclassification of liabilities, taken together, create a significant audit risk that the company's financial outlook may have been presented more favorably than it actually was. In this context, the audit work should focus on the areas summarized in Table 11.4.

Table 11.4. Key Audit Focus Areas Related to Financial Statement Adjustments

Control Area	Scope of Review
Financing expenses	Interest accruals, exchange rate differences, loan agreements, and year-end closing entries
Depreciation and amortization expenses	Fixed assets, special costs, right-of-use assets, and useful life estimates
Debt classification	Short-term and long-term debt distinction, payment schedules, and restructuring terms
Investment expenditures	Capitalized amounts, contract revisions, technical acceptance documents, and board approvals

Related-party transactions	Liabilities to shareholders, capital advances, intra-group settlements, and footnote disclosures
Risk of management override	Manual accounting entries, unusual classifications, and senior management approvals

Overall, the primary purpose of the audit is not merely to test the mathematical accuracy of financial statement items. The auditor should also assess whether financial statement items are fairly presented, whether management has influenced accounting estimates and classification decisions, whether internal control procedures have been overridden, and whether there is a risk of misleading users of the financial statements.

11.4. High-Risk Transaction Areas and Control Weaknesses

The findings in the Kazey A.Ş. case should not be considered merely as isolated accounting errors. The underreporting of financing expenses, the underestimation of depreciation and amortization expenses, the presentation of short-term liabilities as long-term, the capitalization of investment expenditures without sufficient approval, the inadequate disclosure of related-party transactions, and the application of certain deductions without board approval, when considered together, reveal a risk of financial statement manipulation at the senior management level.

Therefore, suspicious areas of trading should be evaluated not only in terms of technical accounting accuracy, but also in terms of management override, financial reporting ethics, internal control deficiencies, audit committee oversight, and the risk of misleading users of financial statements.

11.4.1. Underreporting of Financing Expenses

Kazey A.Ş. reported financing expenses of USD 3,382,000 for 2025. However, the internal audit revealed that USD 173,000 in interest and

exchange rate difference expenses had not been reflected in the year-end financial statements. The effect of this adjustment on financing expenses is summarized in Table 11.5.

Table 11.5. Adjustment of Kazey A.Ş.'s Financing Expenses for Unrecorded Interest and Exchange Rate Differences

Explanation	**Amount (USD)**
Reported financing expenses	3,382,000
Unrecorded interest and exchange rate difference expenses	173,000
Adjusted financing expenses	3,555,000

As shown in Table 11.5, financing expenses are one of the main causes of Kazey A.Ş.'s reported loss. The understatement of this item causes the company's net loss to appear lower than it actually is and creates a more favorable impression of financial sustainability. This situation may mislead lenders, shareholders, potential investors, and other users of the financial statements when evaluating the company's debt burden, repayment capacity, and going concern risks.

From an audit perspective, this finding may also indicate a management tendency to soften financial results or understate the actual amount of losses. Therefore, the auditor should retest all loan agreements, accrued interest calculations, exchange rate difference calculations, payment schedules, and year-end closing entries in order to assess whether financing expenses have been completely, accurately, and fairly presented in the financial statements.

11.4.2. Understatement of Depreciation and Amortization Expenses

Some of the company's investments in marina infrastructure, commercial areas, electrical systems, pier renovations, and technical service capacity in 2025 were capitalized as tangible fixed assets, right-of-use assets, or leasehold improvements. However, the internal audit determined that depreciation and amortization expenses had been

understated for certain assets. The understatement of depreciation and amortization expenses is summarized in Table 11.6.

Table 11.6. Understatement of Depreciation and Amortization Expenses Related to Capitalized Assets

Expense Type	**Understated Amount (USD)**
Amortization expense	56,000
Depreciation expense	72,000
Total expense understatement	**128,000**

This deficiency has a twofold impact on the financial statements. First, the company's net loss is understated because depreciation and amortization expenses were not fully recognized in the income statement. Second, fixed assets, right-of-use assets, and leasehold improvements may be overstated in the statement of financial position because the related accumulated depreciation and amortization amounts were understated. Therefore, depreciation and amortization deficiencies should be evaluated not only as periodic expense recognition errors, but also in terms of asset valuation, financial statement reliability, and the fair presentation of the company's financial position. Accordingly, the auditor should retest the useful lives, depreciation rates, amortization periods, and leasehold improvement amortization schedules of capitalized assets.

11.4.3. Misclassification of Liabilities and Liquidity Risk

The audit revealed that certain foreign currency loans due within 12 months of the balance sheet date had been classified under long-term liabilities. This classification error understates the company's short-term debt repayment pressure. The required reclassification of these liabilities is summarized in Table 11.7.

Table 11.7. Reclassification of Foreign Currency Loans from Long-Term to Short-Term Liabilities

Liability Item	**Reported Classification**	**Required Classification**
USD 4,200,000 loan principal	Long-term debt	Short-term debt
USD 610,000 accrued interest	Long-term debt	Short-term debt

This classification error directly affects the company's current ratio, short-term solvency, and liquidity risk assessment. Presenting short-term liabilities as long-term liabilities makes the company's financial position appear stronger and more sustainable than it actually is. This issue is particularly important for lenders, shareholders, and other users of the financial statements, as it may prevent them from accurately assessing the company's short-term cash needs, debt repayment pressure, and solvency risk. Therefore, the auditor should thoroughly review loan agreements, repayment schedules, accrued interest records, post-balance sheet payment dates, restructuring agreements, and year-end liability classifications to determine whether debt obligations have been properly presented according to their maturity.

11.4.4. Capitalization of Investment Expenditures with Unapproved or Insufficient Documentation

Kazey A.Ş.'s marina renovation and expansion investments for 2025 exceeded their initial budget. Significant variances were identified in certain investment items, as summarized in Table 11.8.

Table 11.8. Budget Variances in Kazey A.Ş.'s Marina Renovation and Expansion Investments for 2025

Investment Item	Initial Budget (USD)	Actual Amount (USD)	Variance (USD)
Commercial area construction	2,100,000	3,220,000	1,120,000
Electricity infra-structure	400,000	586,000	186,000
Pier and technical areas	750,000	920,000	170,000
Total	**3,250,000**	**4,726,000**	**1,476,000**

As shown in Table 11.8, the company's marina renovation and expansion investments exceeded the initial budget by USD 1,476,000. Exceeding the initial investment budget does not, by itself, indicate fraud. However, capitalizing additional works without a board decision, contract revision, technical acceptance report, or sufficient supporting documentation constitutes a significant control weakness.

This risk has two main implications. First, the period loss may be understated if expenditures that should have been recognized as expenses were improperly capitalized. Second, management may have bypassed budgetary controls through unauthorized or inadequately documented investment expenditures. Therefore, the auditor should examine all high-value capitalized investment expenditures on a document-by-document basis by testing the consistency among contracts, additional work orders, technical acceptance reports, invoices, payments, and board approvals.

11.4.5. Discount Practices and Revenue Management Risks

The case revealed that some marina mooring fees included seasonal and agency discounts; however, there was no written pricing policy, board decision, or explicit approval within the authorization matrix for all discounts.

Discounts applied without board approval pose a risk to the completeness and accuracy of revenues. Such discounts may result in preferential treatment for certain customers, loss of revenue, unauthorized discounting, or the transfer of indirect benefits to related parties.

Therefore, discount practices should be evaluated not only as a commercial decision but also as a risk of revenue management and control deficiencies. The auditor should examine the compliance of discounts with the written pricing policy, their customer-based distribution, authorization approvals, and related party connections.

11.4.6. Related Party Transactions and Lack of Transparency

Kazey A.Ş.'s financial statements do not adequately detail liabilities to partners, capital advances, accrued interest, offsetting transactions with group companies, and related party financial transactions.

Related-party transactions are a high-risk area for financial statement manipulation because intra-group transactions can influence financial results by manipulating liabilities, receivables, financing expenses, accrued interest, or income/expense classifications.

Therefore, related party transactions should be evaluated not only through accounting records but also in terms of economic substance, market conformity, independent certification, counterparty reconciliation, and footnote disclosures. Insufficient disclosure prevents users of financial statements from seeing the company's true financial relationships and risks.

11.4.7. Ethics, Management override, and Red Flags

In the case of Kazey A.Ş., management override is central to the audit risk. Management override occurs when senior management influences the financial reporting process by bypassing normal internal control procedures or directing accounting decisions. This may take the form of explicit fraud, but it may also occur in more subtle ways, such as leaving expenses unrecorded, misclassifying liabilities,

overstating assets, or providing insufficient disclosures. The main red flags identified in this case are summarized in Table 11.9.

Table 11.9. Red Flags Indicating Management Override Risk in Kazey A.Ş.

Red Flag	**Explanation**
High financing costs	The financing burden is the main reason for the company's losses
Unrecorded interest and exchange rate differences	Net loss has been understated
Understated depreciation and amortization expenses	Assets may be overstated and expenses understated
Short-term debt classified as long-term debt	Liquidity risk may be concealed
Lack of written approval	Additional investment expenditures are not adequately documented
Discounts granted without board approval	Risk of revenue loss and unauthorized transactions
High volume of related-party transactions	Financial results may be influenced by intra-group transactions
Manual accounting entries	Risk of management override increases
Understatement of losses	Users of the financial statements may be misled

When these red flags are considered together, the issue in this case is not merely a technical accounting error. The primary audit risk is that senior management may have influenced accounting records, classifications, estimates, and disclosures in order to present the company's financial results more favorably than they actually were. This situation also has serious consequences in terms of financial reporting ethics. The principles of honesty, impartiality, transparency, accountability, professional diligence, and reliability may be compromised. Management is obligated to provide users of financial statements with truthful, complete, and understandable information. When this obligation

is not fulfilled, financial statements cease to be a decision-making tool and become merely a tool to support management objectives.

11.4.8. Internal Control and Audit Committee Weaknesses

The case demonstrates that the internal control system at Kazey A.Ş. is not sufficiently robust, particularly in relation to management decisions and financial reporting processes. Key examples of these weaknesses include the de facto implementation of transactions requiring board approval through management decisions, weak year-end closing controls, insufficient review of debt classifications, and the lack of independent review over related-party transactions. The main internal control weaknesses are summarized in Table 11.10.

Table 11.10. Internal Control Weaknesses Related to Management Override Risk in Kazey A.Ş.

Control Area	Current Weakness	Risk
Management approval controls	Additional investment expenditures and discounts are not supported by sufficient written approval	Risk of unauthorized transactions and budget overruns
Accounting closing controls	Interest, exchange rate differences, depreciation, and amortization records have not been fully reviewed	Risk of understated expenses and inaccurate financial results
Debt classification controls	Short-term liabilities have not been properly distinguished from long-term liabilities	Risk of concealed liquidity pressure
Related-party controls	The independent review mechanism for intra-group transactions is weak	Risk of reduced transparency and conflicts of interest
Manual accounting entry controls	There is no strong approval mechanism to limit senior management override	Risk of management override
Audit committee oversight	Critical accounting estimates have not been sufficiently challenged	Risk of unreliable financial reporting

These control weaknesses demonstrate that management override risk is not related solely to individual accounting decisions, but also

to weaknesses in the company's corporate governance structure. Therefore, audit committee oversight at Kazey A.Ş. should be strengthened, manual accounting entries should be subject to independent verification, a year-end closing checklist should be implemented, and related-party transactions should be reported regularly.

11.5. Potential Executive-Level Financial Reporting Manipulation Scenario

The Kazey A.Ş. case do not, by themselves, mean that every accounting entry was intentionally misrepresented. However, when considered together, the underreporting of financing expenses, the underestimation of depreciation and amortization expenses, the presentation of short-term liabilities as long-term, the capitalization of investment expenditures without sufficient documentation and approval, the limited disclosure of related-party transactions, and the application of certain deductions outside the scope of written authorization, reveal a risk of financial statement manipulation at the senior management level.

According to a possible scenario, Kazey A.Ş. 's senior management may have wanted to present a more positive financial statement in 2025 due to high capital expenditures, foreign currency borrowing, financing expenses, liquidity pressures, and a net loss for the period. The company's reported net loss for the period is 2,635,000 USD. However, considering underrecognized amortization expense, underretirement expense, and unrecorded interest/exchange rate difference expense, the adjusted net loss for the period is expected to be approximately 2,936,000 USD. This indicates that the company's loss may be approximately 301,000 USD higher than reported.

In this scenario, the first area of risk is financing expenses. Since a significant portion of the company's loss stems from financing expenses, the failure to recognize USD 173,000 in interest and exchange rate expenses has made the financial performance appear better than it actually is. This practice may underestimate the company's

borrowing costs and period loss, leading financial statement users to underestimate the company's true financial burden.

In this scenario, several financial reporting risks require careful audit attention. A significant concern relates to financing expenses, since a substantial portion of the company's loss is associated with borrowing costs. The non-recognition of USD 173,000 in interest and foreign exchange expenses may have resulted in a more favorable presentation of financial performance than the underlying economic reality would support. Such an omission may understate both the company's financing burden and its period loss, causing financial statement users to form an incomplete view of the entity's actual financial pressure.

Another important risk concerns the recognition of amortization and depreciation expenses. Certain investments made during 2025 were capitalized as tangible fixed assets, right-of-use assets, or special costs. However, the under-allocation of USD 56,000 in amortization expense and USD 72,000 in depreciation expense indicates that the related assets may not have been expensed in accordance with their consumption of economic benefits. This situation affects both the income statement and the balance sheet, as expenses are understated while asset values are overstated. As a result, the company's reported loss may appear lower and its asset position stronger than is actually the case.

The classification of liabilities also creates a material presentation risk. The classification of a USD 4,200,000 loan principal and USD 610,000 of accrued interest due within twelve months after the balance sheet date as long-term liabilities may conceal the company's short-term liquidity pressure. Such a presentation can make indicators such as the current ratio and short-term solvency position appear more favorable than they are. This is particularly significant for lenders, investors, and business partners who rely on financial statements to assess the company's repayment capacity and liquidity risk.

Capitalization of investment expenditures represents another area requiring professional skepticism. Kazey A.Ş. incurred budget overruns in certain marina renovation and expansion investments. However,

the capitalization of these additional expenditures as assets should be questioned where there is no board resolution, contract revision, technical acceptance report, or sufficient supporting documentation confirming the nature and necessity of the additional works. If expenditures that should have been recognized as period expenses are capitalized, the company's period loss may be understated and the fair presentation of the financial statements may be impaired.

Related-party transactions and discounting practices also raise transparency and completeness concerns. If debts to shareholders, capital advances, offsetting transactions with group companies, and accrued interest are not disclosed adequately, users of financial statements may be unable to evaluate the company's actual financial relationships and dependency structure. Similarly, discounts granted without a board decision or a written pricing policy may create risks regarding the objectivity, consistency, and completeness of revenue recognition. These practices may also raise concerns about customer-based fairness and the reliability of reported sales figures.

In this scenario, the ethical problem is not simply the erroneous accounting entries. The real ethical issue is whether senior management has acted honestly, impartially, transparently, and accountably towards users of the financial statements. Financial statements are a decision-making tool for partners, lenders, suppliers, employees, and other stakeholders. Therefore, understating losses, misclassifying liabilities, or inadequately disclosing related-party transactions can result in misleading users of the financial statements.

This structure should not be considered direct, definitive proof of fraud. However, when the identified indicators are considered together, there is a significant risk that the financial statements may have been influenced by management preferences. In particular, high financing pressure, the desire to portray the investment project as successful, the need to present a stronger balance sheet to lenders, and the perception of management performance are all factors that increase the risk of manipulation at the senior management level.

Therefore, the auditor's primary priority is not to simply accept management's statements, but to test the financial statement items with

independent evidence. The auditor should recalculate financing expenses, review depreciation and amortization records, reassess the maturity classification of liabilities, examine approval and technical acceptance documents for investment expenditures, analyze related party transactions in detail, and assess whether management has exceeded internal control processes.

In conclusion, the potential manipulation scenario in the Kazey A.Ş. case unfolds not so much through directly increasing revenues, but rather through downplaying losses, overstating assets, concealing short-term debt pressure, and providing limited disclosure of related-party transactions. Therefore, the case demonstrates that financial manipulation at the senior management level can occur not only through overt fraud, but also through accounting estimates, classification preferences, incomplete records, and inadequate disclosure.

11.6. Audit Procedures, Data Analytics and Control Evaluation

In the case of Kazey A.Ş., the audit should not be limited to checking the mathematical accuracy of accounting records. The auditor should independently examine, with supporting evidence, areas where senior management may have interfered with the financial reporting process. Therefore, audit procedures should be designed around financing expenses, depreciation and amortization calculations, liability classification, capital expenditures, related party transactions, manual accounting entries, and audit committee oversight.

The audit procedures, data analytics tests, and control assessments to be applied in this section are discussed under the following headings.

11.6.1. Financing Cost Tests

Financing expenses are one of the most significant items directly impacting Kazey A.Ş. 's period loss. Therefore, the auditor should thoroughly verify that reported financing expenses are fully and accurately recorded.

The auditor should first obtain all loan agreements, payment schedules, interest rates, foreign currency loan details, and bank statements. Interest and exchange rate difference expenses that should have accrued at year-end should then be recalculated independently. This recalculation should be compared with the financing expenses recorded in the company's accounting records. The main audit procedures for testing financing expenses are summarized in Table 11.11.

Table 11.11. Audit Procedures for Testing Financing Expenses and Foreign Currency Loan Valuation

Procedure	Audit Objective
Review of loan agreements	To verify interest rates, maturity dates, and payment terms
Recalculation of accrued interest	To determine whether any financing costs have been omitted
Testing of exchange rate calculations	To verify whether foreign currency loans have been correctly valued
Verification of payments with bank statements	To confirm the authenticity of recorded interest and principal payments
Review of year-end closing entries	To identify unrecorded interest and exchange rate difference expenses

The purpose of these procedures is to determine whether the unrecorded interest and exchange rate difference expense of USD 173,000 represents an isolated accounting error or a systematic understatement of financing expenses intended to reduce the reported loss.

11.6.2. Depreciation and Amortization Tests

In Kazey A.Ş.'s financial statements, fixed assets, leasehold improvements, and right-of-use assets constitute a significant portion of the company's statement of financial position. Therefore, the accurate

calculation of depreciation and amortization expenses is critical for both the income statement and the balance sheet.

The auditor should compare fixed asset records with accounting records, investment invoices, technical acceptance reports, contracts, and dates of commencement of use. In addition, useful life estimates, depreciation rates, and amortization periods for leasehold improvements should be re-evaluated. The main audit procedures for testing depreciation and amortization expenses are summarized in Table 11.12.

Table 11.12. Audit Procedures for Testing Depreciation and Amortization Expenses of Capitalized Assets

Procedure	Audit Objective
Comparison of the fixed asset register with accounting records	To verify the accuracy and completeness of capitalized assets
Review of useful life estimates	To evaluate whether depreciation calculations are reasonable
Recalculation of depreciation and amortization expenses	To determine whether any expense amounts have been omitted
Comparison of leasehold improvements with lease or usage periods	To verify whether the amortization period has been correctly determined
Document-by-document review of capitalized expenditures	To test whether expenditures that should have been expensed were improperly capitalized as assets

These procedures should be used to determine the financial statement impact of the USD 56,000 amortization expense understatement and the USD 72,000 depreciation expense understatement. The auditor should assess whether these deficiencies represent isolated calculation errors or indicate a broader weakness in asset capitalization, useful life estimation, and period-end expense recognition controls.

11.6.3. Debt Classification Tests

Correctly classifying liabilities as short-term or long-term directly impacts a company's liquidity and financial sustainability. In the case of Kazey A.Ş. , classifying some short-term liabilities as long-term may have made the company appear to have stronger short-term solvency than it actually did.

The auditor should identify all loan repayment schedules and principal and interest payments due within 12 months of the balance sheet date. These obligations should be classified as short-term liabilities in the financial statements. The main audit procedures for testing debt maturity classification are summarized in Table 11.13.

Table 11.13. Audit Procedures for Testing Short-Term and Long-Term Debt Classification

Procedure	Audit Objective
Obtaining loan repayment schedules	To identify debt obligations falling due within 12 months
Performing a 12-month post-balance-sheet payment analysis	To test whether short-term debts have been correctly classified
Review of restructuring agreements	To determine whether a valid agreement affects the classification of liabilities
Checking post-balance-sheet payments	To verify short-term payment obligations
Recalculation of financial ratios	To measure the impact of misclassification on the current ratio and liquidity indicators

These procedures should determine whether the USD 4,200,000 loan principal and USD 610,000 accrued interest have been classified according to their correct maturity. If these obligations are due within 12 months of the balance sheet date, they should be presented as short-term liabilities rather than long-term liabilities.

11.6.4. Investment Expenditures and Capitalization Tests

Kazey A.Ş.'s investments for 2025 have exceeded its initial budget. Therefore, it must be tested whether the capitalized investment expenditures actually qualify as assets and whether they are supported by the necessary approvals. The auditor should review investment expenditures on a project-by-project basis by testing the consistency among the initial budget, actual expenditures, contracts, additional work orders, technical acceptance reports, invoices, payment documents, and board approvals. The main audit procedures for testing investment expenditures and capitalization decisions are summarized in Table 11.14.

Table 11.14. Audit Procedures for Testing Investment Expenditures and Capitalization Decisions

Procedure	Audit Objective
Comparison of the investment budget with actual expenditures	To identify budget overruns and unusual deviations
Review of contracts and additional work orders	To test whether the expenditure is based on a valid contractual basis
Review of technical acceptance reports	To verify whether the expenditure relates to work that has actually been completed
Review of board approvals	To identify the risk of authority override or unauthorized investment expenditures
Evaluation of capitalization criteria	To test whether expenditures have been appropriately capitalized as assets or should have been recognized as period expenses

These procedures are particularly important for determining whether investment expenditures were properly capitalized or whether certain costs should have been recognized as period expenses. The auditor should also assess whether budget overruns and additional works were supported by valid approvals and sufficient documentation.

11.6.5. Discount Practices and Revenue Control Tests

Kazey A.Ş. , seasonal and agency discounts have been applied to some marina mooring fees. However, there is no written pricing policy or

board approval for all discounts. Therefore, the auditor should test whether the discount applications comply with the authorization and approval matrix. The main audit procedures for testing discount practices are summarized in Table 11.15.

Table 11.15. Audit Procedures for Testing Discount Practices and Approval Controls

Procedure	Audit Objective
Review of pricing policies	To determine whether discounts are based on written rules
Preparation of a customer-based discount list	To test whether specific customers receive unusual advantages
Authorization matrix review	To evaluate whether the person approving the discount is properly authorized
Review of related-party connections	To test whether discounts are granted in favor of intra-group or related parties
Calculation of revenue loss impact	To determine the financial impact of unauthorized discounts

These procedures should be used to determine whether discount practices are based on valid commercial grounds or whether they result from uncontrolled discretionary decisions by management. The auditor should also assess whether unauthorized discounts have caused revenue loss, weakened pricing discipline, or created a risk of preferential treatment for specific customers or related parties.

11.6.6. Related Party Transaction Tests

Related-party transactions are among the high-risk areas for financial statement manipulation. Therefore, liabilities to shareholders, capital advances, offsets with group companies, accrued interest, and other related-party transactions should be examined thoroughly. The main audit procedures for testing related-party transactions are summarized in Table 11.16.

Table 11.16. Audit Procedures for Testing Related-Party Transactions and Disclosure Adequacy

Procedure	**Audit Objective**
Preparation of a related-party list	To ensure the complete identification of all related parties
Analysis of intra-group debts and receivables	To determine whether financial results were influenced by intra-group transactions
Obtaining counterparty confirmations	To support the accuracy of balances with external evidence
Review of interest and offsetting transactions	To assess whether transactions are consistent with market conditions
Review of footnote disclosures	To evaluate whether sufficient transparency is provided to users of the financial statements

In related-party transactions, the auditor should focus not only on the accounting entries, but also on the economic substance of the transactions, their conformity with market conditions, and the adequacy of disclosures. This review is particularly important because related-party transactions may be used to shift liabilities, defer losses, influence profitability, or obscure the company's actual financial position.

11.6.7. Management override and Manual Record Tests

Manual journal entries are particularly important in assessing the risk of financial manipulation at the senior management level. The auditor should analyze journal entries, especially those recorded near year-end, that involve unusually round amounts, weak explanations, unusual classifications, or entries created under senior management instruction. The main analytical tests for reviewing manual journal entries are summarized in Table 11.17.

Table 11.17. Analytical Tests for Reviewing Manual Journal Entries and Management Override Risk

Analytical Test	Audit Objective
Year-end manual journal entry analysis	To identify unusual entries recorded during the closing period
Round-amount entry test	To identify artificial or unsupported journal entries
Weak-description entry test	To identify entries with unclear transaction explanations
Senior management user-code analysis	To detect entries created or approved through senior management access
Reversing entry analysis	To identify temporary, corrective, or period-shifting entries
Unusual classification test	To identify abnormal movements in liability, expense, or asset accounts

These tests reduce reliance on management representations and enable the auditor to reach an independent, evidence-based conclusion regarding whether manual journal entries were used to influence financial results, shift expenses between periods, misclassify liabilities, or present the company's financial position more favorably than it actually was.

11.6.8. Internal Control and Audit Committee Evaluation

In the case of Kazey A.Ş., the control assessment should focus particularly on management override risk. Even if formal internal control procedures are in place, the control environment cannot be considered effective if senior management is able to circumvent these controls. The key control areas to be evaluated are summarized in Table 11.18.

Table 11.18. Control Environment Assessment for Management Override Risk in Kazey A.Ş.

Control Area	Evaluation Criteria
Board of directors' approvals	Are large-scale investment, borrowing, and discount transactions subject to written approval?
Audit committee oversight	Are critical accounting estimates and classifications independently challenged?
Manual journal entry controls	Are unusual accounting entries subject to second-level approval?
Year-end closing controls	Are interest, exchange rate differences, depreciation, amortization, and debt classifications tested using a checklist?
Related-party controls	Are intra-group transactions subject to independent review and disclosure procedures?
Ethical reporting mechanism	Can employees safely report pressure to engage in improper financial reporting?

If this assessment reveals that the control environment against management override is inadequate, the auditor should report the findings directly to the board of directors or the audit committee. This is particularly important because weaknesses in this area may allow senior management to influence accounting estimates, classifications, disclosures, and period-end financial reporting decisions.

11.6.9. Proposed Control Matrix

For Kazey A.Ş., the following control matrix should be implemented to reduce financial reporting risks and management override risk. The matrix links each identified risk to a recommended control activity, control type, and responsible unit, as summarized in Table 11.19.

Table 11.19. Recommended Control Matrix for Reducing Financial Reporting and Management Override Risks in Kazey A.Ş.

Risk	Recommended Control	Control Type	Responsible Unit
Understatement of financing expenses	Year-end recalculation of interest and exchange rate differences	Detective	Accounting / Finance
Understatement of depreciation and amortization expenses	Fixed asset and leasehold improvement depreciation checklist	Detective	Accounting
Presentation of short-term debt as long-term debt	Debt classification check based on a 12-month repayment schedule	Preventive / Detective	Finance
Capitalization of unauthorized investment expenditures	Board approval and technical acceptance certificate requirement	Preventive	Board of Directors / Finance
Unauthorized discount application	Written pricing policy and discount authorization matrix	Preventive	Sales / Finance
Insufficient disclosure of related-party transactions	Related-party confirmation and footnote disclosure control procedure	Detective	Accounting / Legal
Management override	Independent second-level verification for manual journal entries	Preventive	Audit Committee
Pressure for unethical financial reporting	Anonymous ethics reporting hotline	Reporting / Monitoring	Audit Committee / Internal Audit

This control matrix aims not only to correct identified accounting errors, but also to structurally reduce management override risk. Accordingly, preventive controls should limit unauthorized decisions before they affect the accounting records, while detective and monitoring controls should support independent review, transparency, and timely identification of financial reporting irregularities.

11.6.10. General Assessment

Overall, the primary purpose of the audit procedures in the case of Kazey A.Ş. is not simply to test the accuracy of the records. The auditor should assess whether the financial statements are overstated by management, whether accounting estimates are reasonable, whether liability classifications reflect reality, and whether related-party transactions are disclosed transparently.

In this context, the audit work should be supported by technical accounting tests, data analytics, document verification, management approval review, related party reconciliations, and audit committee oversight. Otherwise, the risk of management override could seriously weaken the credibility of the financial statements and the company's ethical control environment.

11.7. Findings, Auditor's Assessment and Recommendations

The review of Kazey A.Ş.'s financial statements as of December 31, 2025, identified significant audit findings related to financing expenses, depreciation and amortization calculations, debt classification, capital expenditures, discount applications, and related party transactions. Considered collectively, these findings indicate that the company's financial position may have been presented more favorably than its actual condition and may also point to a risk of senior management override in the financial reporting process.

Table 11.20. Summary of Key Audit Findings and Management Override Risk Indicators in Kazey A.Ş.

No	Finding	Auditor's Assessment	Suggestion
1	Financing expenses were under-recorded. It was determined that an expense of 173,000 USD was not reflected in the financial statements during year-end interest and exchange rate calculations.	Financing expenses are one of the most significant items directly affecting a company's net loss for the period. Failure to record this expense leads to an underestimation of the net loss and an incomplete assessment of the company's borrowing costs by financial statement users.	All loan agreements, payment schedules, interest rates, and exchange rate calculations must be reviewed. Unrecognized interest and exchange rate expenses of USD 173,000 should be recognized; and a mandatory recalculation of financing expenses should be implemented at year-end closing.
2	Depreciation and amortization expenses were under-allocated. It was determined that a total of 128,000 USD in depreciation and amortization expenses were not recorded.	Underestimation of depreciation and amortization expenses leads to an underestimation of losses in the income statement and an overestimation of fixed assets and special costs in the balance sheet. This constitutes not only a periodic expense error but also a significant risk to asset valuation and the reliability of financial statements.	All fixed assets, rights-of-use assets, and special cost accounts should be reviewed. Useful lives, depreciation rates, and amortization periods should be reassessed; the underrecognition of USD 56,000 amortization expense and USD 72,000 depreciation expense should be recognized.
3	Short-term liabilities were presented as long-term. It was determined that the total principal and interest accruals of the loan, amounting to 4,810,000 USD were shown under long-term liabilities instead of short-term liabilities.	This classification error underestimates the company's short-term liquidity pressure. Presenting short-term debt as long-term can mislead assessments of current ratios, solvency, and going concern.	Loan repayment schedules should be re-analyzed as of the balance sheet date, and debts due within 12 months of the balance sheet date should be transferred to short-term liabilities. A year-end closing checklist should be created for debt classification.

4	There are missing approvals and documentation for investment expenditures. For some additional investment expenditures, board approval, contract revision, additional work order, or technical acceptance report is missing.	Capitalizing investment expenditures without sufficient approval and documentation creates the risk of recording expenses that are actually deductible as assets. This can reduce the net loss for the period, overestimate fixed assets, and weaken budget overrun control.	Capitalized investment expenditures should be reviewed on a project-by-project basis. Expenditures lacking board approval, contract revisions, additional work orders, technical acceptance reports, and payment documents should be reclassified; expense adjustments should be made where necessary.
5	Discount applications are not based on sufficient approval. Seasonal and agency discounts have been applied to some marina mooring fees; however, there is no written pricing policy or board decision for all discounts.	Unauthorized or undocumented discounts create risks to the completeness, accuracy, and impartiality of revenues. This practice increases the likelihood of preferential treatment for certain customers, revenue loss, transfer of indirect benefits to related parties, or revenue management at management discretion.	All discounts must be applied within the scope of the written pricing policy and authorization matrix. Discount rates, customer-specific discount lists, and approval documents should be reviewed regularly; discounts requiring board approval should be blocked systemically.
6	There is insufficient disclosure in related party transactions. Liabilities to partners, capital advances, accrued interest, and offsetting transactions with group companies are not disclosed in sufficient detail in the financial statements.	Related-party transactions represent a high-risk area in terms of influencing financial results through intra-group transactions. Insufficient disclosure makes it difficult for users of financial statements to assess the company's true debt relationships, financing structure, and conflict of interest risks.	Related party transactions should be listed in detail, counterparty reconciliations should be obtained, and a market compliance assessment should be conducted. Liabilities to partners, capital advances, accrued interest, and offsetting transactions should be clearly reported in the footnotes to the financial statements.
7	Control mechanisms against management	This finding reinforces all other findings in the case	Manual accounting entries, high-value capital

	override are inadequate. There is insufficient oversight by the independent audit committee over manual accounting records, investment approvals, discount applications, and critical classification decisions.	regarding a fundamental control weakness. The influence of senior management on accounting estimates, classifications, and approval processes poses a serious risk to the objectivity and reliability of the financial statements.	expenditures, debt classifications, related-party transactions, and unusual discounts must be subject to independent second-level approval. The audit committee should regularly review year-end closing entries and critical accounting decisions.

Overall, not all findings identified at Kazey A.Ş. . should be interpreted as direct and definitive evidence of fraud. However, the underreporting of financing expenses, the underestimation of depreciation and amortization expenses, the presentation of short-term liabilities as long-term, the capitalization of investment expenditures without sufficient documentation, the application of discounts outside the scope of authorization, and the inadequate disclosure of related parties, when considered together, pose a significant audit risk that the financial statements may have been presented more favorably than they actually are.

Therefore, the auditor's primary priority is not merely to correct individual accounting entries. The auditor should also assess the risk of management override, financial reporting ethics, audit committee oversight, and the independence of the internal control system. Financial statement adjustments should be made, the control environment strengthened, and management decisions subjected to stricter scrutiny.

11.8. Instructor Notes

This case is designed to help students assess financial statement manipulation not only through overt forgery or falsification of documents, but also through management override, accounting estimates, classification decisions, incomplete expense recording, and inadequate disclosure. In the case of Kazey A.Ş. , the key issue is not

whether certain financial statement items are recorded, but rather whether management may have manipulated these items to present a more favorable financial outlook for the company.

Students should be expected to discuss issues such as the underreporting of financing expenses, the underestimation of depreciation and amortization expenses, the misrepresentation of short-term liabilities as long-term, the capitalization of investment expenditures without sufficient documentation, and the limited disclosure of related-party transactions. Each of these elements may appear as a technical accounting error on its own; however, when considered together, they strengthen the risk of financial statement manipulation at the senior management level.

This case demonstrates that the risk of management override should be specifically addressed in the audit process. The auditor should not rely solely on management disclosures; they should recalculate financing expenses, test the maturity classification of liabilities, examine the approval and documentation support for capital expenditures, and thoroughly evaluate manual accounting entries.

During the teaching process, students should be expected to analyze each finding at three levels: the impact of technical accounting, the impact on users of financial statements, and the ethical/control dimension. For example, presenting short-term liabilities as long-term is not only a classification error; it is also a financial reporting problem that conceals a company's liquidity risk and can influence lenders' decisions.

In conclusion, the case of Kazey A.Ş. demonstrates that the reliability of financial reporting is not simply a matter of accurate record-keeping. Integrity, transparency, impartiality, accountability, audit committee oversight, and a strong internal control environment must be considered together for the reliability of financial statements.

11.9. Discussion Questions

1. Kazey A.Ş. is the risk of management override most evident?
2. How does underreporting financing expenses affect a company's net loss and financial outlook?
3. What are the consequences of under-allocating depreciation and amortization expenses, both for the income statement and the balance sheet?
4. Which financial ratios and user decisions can be misled by presenting short-term debt as long-term?
5. What audit risks arise from capitalizing investment expenditures without sufficient documentation and board approval?
6. How should discount applications made without a board decision be evaluated in terms of revenue accuracy and internal control systems?
7. Why are related-party transactions considered high-risk for financial manipulation at the senior management level?
8. How can the line between financial reporting error and ethical violation be drawn in this case?
9. Why should an auditor not rely solely on management statements?
10. In the case of Kazey A.Ş., in which areas should the supervisory committee provide more active oversight?
11. In what ways might financial statement users have been misled in this case?
12. What should be the top three recommended check-ups at Kazey A.Ş. to reduce the risk of management override ?

11.10. Conclusion

The Kazey A.Ş. case demonstrates that financial statement manipulation at the senior management level does not always manifest as overt fraud. Underreporting financing expenses, underestimating depreciation and amortization expenses, presenting short-term liabilities as long-term, capitalizing

investment expenditures without sufficient documentation, and under-disclosure of related-party transactions are also significant risk areas that can mislead users of financial statements.

The audit revealed that the company's reported net loss for the period is lower than its adjusted loss. Considering the underrecognized amortization expense, underreported depreciation expense, and unrecorded interest/exchange rate expenses, the company's loss is expected to be approximately 301,000 USD higher than reported. This indicates that the financial statements do not fully reflect the company's true performance and financial burden.

The case also has significant implications for debt classification and liquidity risk. Classifying debts due within 12 months of the balance sheet date as long-term debt makes the company's short-term solvency appear more favorable than it actually is. Such classification errors create a risk of misleading information, particularly for lenders, partners, and investors.

The main recommendation for Kazey A.Ş. is not simply to correct the identified accounting errors. The company needs to establish a stronger control environment that limits management override in its financial reporting process. This includes strengthening year-end closing controls, subjecting manual accounting entries to independent approval, making board approval and technical acceptance documents mandatory for capital expenditures, providing detailed disclosure of related party transactions, and having the audit committee regularly review critical accounting decisions.

Overall, the Kazey A.Ş. case offers important lessons regarding financial reporting reliability, management ethics, and internal control systems. Financial statement manipulation can occur not only through inflating revenues but also through minimizing losses, deferring expenses, misclassifying liabilities, and understating disclosures. Therefore, the auditor should evaluate accounting choices at the senior management level with professional skepticism and test, with independent evidence, whether the financial statements are presented fairly.

Appendix 11.1. Audit Questionnaire

Kazey A.Ş. Executive-Level Financial Manipulation Questionnaire Form

No	Area of Control	Question	Objective / Audit Risk
1	Financial Reporting	Were significant accounting estimates in the preparation of the financial statements guided by senior management?	Assessing the risk of management override.
2	Financing Expenses	Have all loan agreements, interest rates, and payment schedules been compared with accounting records?	Identifying the risk of underfunding costs.
3	Interest Accruals	Have the interest expenses that were due to accrue as of December 31, 2025 been recalculated?	To identify unrecorded interest expenses.
4	Exchange Rate Difference Expenses	Have exchange rate difference calculations related to foreign currency debts been independently tested?	Assessing the risk of underreporting exchange rate losses.
5	Financing Expense Adjustment	Has a correction entry been proposed for the unrecorded interest/exchange rate difference expense of 173,000 USD?	To ensure that net loss is accurately reported.
6	Depreciation	Have the depreciation calculations for fixed assets been re-tested in terms of useful life and rates?	To identify the risk of under-depreciation expense.
7	Amortization Expenses	Are the amortization periods for special costs and right-of-use assets consistent with the contract term?	Assessing the risk of underpayment of amortization and high asset value.

No	Area of Control	Question	Objective / Audit Risk
8	Activation	Do capitalized investment expenditures truly constitute assets?	Identifying the risk of recording expenses as assets.
9	Investment Documents	Do you have invoices, contracts, additional work orders, and technical acceptance reports for high-value investment expenditures?	Identifying the risk of activation without documentation or adequate support.
10	Board of Directors Approval	Have the investment expenditures that resulted in the budget overrun been approved by the board of directors?	Assessing the risk of unauthorized investment and overcontrol.
11	Budget Deviation	Have the initial budget and actual investment expenditures been compared?	Identifying unusual cost increases.
12	Debt Classification	Are liabilities payable within 12 months of the balance sheet date shown as short-term liabilities?	To identify the risk of concealment of liquidity risk.
13	Loan Principal	Has it been verified that the 4,200,000 USD loan principal is classified under the correct maturity?	To test the risk of misrepresenting short-term debt as long-term.
14	Interest Accrual Classification	Has it been verified that the 610,000 USD in interest accrual was reported for the correct maturity date?	Identifying debt classification errors.
15	Financial Ratios	Has the impact of debt classification errors on current ratio and liquidity indicators been calculated?	Assessing the risk of misleading users of financial statements.
16	Discount Policy	Are the discounts applied to marina mooring fees based on a written pricing policy?	Identifying the risk of unauthorized discounts and loss of revenue.

No	Area of Control	Question	Objective / Audit Risk
17	Authorization Matrix	Have the authority limits of those approving the discounts been checked?	Assessing revenue management risks that are outside of management control.
18	Customer-Based Discounts	Have discounts been analyzed on a customer-by-customer basis to identify unusual concentrations of interest?	Identifying the risk of granting preferential treatment to certain customers.
19	Related Parties	Are the partners, group companies, and management-related parties fully listed?	To reduce the risk of under-disclosure of related-party transactions.
20	Intra-Group Operations	Have the debt, receivables, offsetting, and interest transactions with the group companies been analyzed?	To identify the risk of financial results being influenced by intra-group transactions.
21	Agreement of the Other Party	Has counterparty reconciliation been obtained for related party balances?	To support the accuracy of the balances with external evidence.
22	Footnote Explanations	Are related-party transactions disclosed in sufficient detail in the footnotes to the financial statements?	Assessing the risks of transparency and reliable reporting.
23	Manual Accounting Records	Have the manual accounting entries made near the end of the year also been reviewed?	Identifying the risk of management override.
24	Unusual Records	Have accounting vouchers with rounded-out consistency, poor explanations, or reversed entries been analyzed?	Identifying artificial or period-shifted records.
25	Management Instructions	Are adjustments made to accounting records at the instruction of senior management tracked separately?	Assessing the risk of management override .

No	Area of Control	Question	Objective / Audit Risk
26	Audit Committee	Have the critical accounting estimates and classification decisions been reviewed by the audit committee?	To identify the lack of independent oversight.
27	Closing Controls	Does the year-end closing checklist include financing expenses, depreciation, amortization, and debt classification?	To reduce errors in year-end financial reporting.
28	Ethical Statement	Is there an ethics reporting hotline where employees can securely report pressures related to financial reporting?	To ensure that unethical instructions are reported.
29	Financial Statement Adjustments	Have the necessary corrective entries been made for missing expenses and incorrectly classified liabilities?	To ensure a fair and accurate presentation of financial statements.
30	Overall Conclusion	When the identified errors are considered together, is there a risk of financial statement manipulation at the senior management level?	To evaluate the impact of the findings on the audit report, the control environment, and management actions.

PART IV

FUTURE OF INTERNAL AUDIT

Chapter 12- Continuous Auditing and Real-Time Assurance

Introduction

Digitalization has significantly transformed the scope, timing, and assurance-generating methods of the internal audit function. In businesses, financial transactions, operational processes, user access, customer movements, supply chain activities, and cybersecurity incidents now largely occur through digital systems. This structure necessitates that auditing move beyond being merely a retrospective review at the end of a period; it requires a transformation into a more continuous, data-driven, technology-supported, and risk-based assurance mechanism.

Continuous auditing and real-time assurance are central to this transformation. While the traditional audit model is largely based on sample-based and periodic checks, the continuous auditing model enables more frequent or real-time monitoring of transaction data, control deviations, system logs , anomaly indicators, and risk signals. This allows the auditor to assess errors, irregularities, control breaches, or cybersecurity risks not only at the end of the period but also at the time or shortly after they arise.

This section discusses continuous control monitoring, real-time audit systems, intelligent dashboards, and integrated assurance models. Continuous control monitoring involves the automated monitoring of critical control points; real-time audit systems enable the real-time analysis of process and system data; intelligent dashboards allow for the management of audit findings and risk indicators; and integrated assurance models refer to the coordinated operation of internal audit, risk management, compliance, information security, and management oversight functions.

The main objective of this chapter is to demonstrate that continuous auditing is not merely a technical automation application. An effective

continuous auditing model should encompass reliable data sources, correctly defined control rules, meaningful alert thresholds, explainable analytical models, qualified audit teams, a strong governance structure, and internal audit independence. Otherwise, systems can become mere technical tools that generate numerous alerts but offer limited real assurance value.

In this context, the chapter aims to enable students and practitioners to consider continuous auditing as a strategic component of modern internal auditing. Continuous auditing has the potential to expand the scope of transactions, identify risks early, produce audit evidence in a timely manner, monitor management actions, and provide the audit committee with more up-to-date assurance. However, risks such as data quality, system integration, false positive alerts, explainability of AI models , over-reliance on automated outputs by the auditor, and maintaining the limits of independence must be carefully managed.

12.1. Continuous Control Monitoring

Digitalization has fundamentally changed the timing logic of the audit function. While the traditional audit approach mostly relied on periodic, sample-based, and retrospective reviews, the increasing transaction volume in today's businesses, the execution of processes through ERP, cloud, artificial intelligence, and automation systems, has made it necessary for audits to be more frequent, systematic, and technology-supported. At the heart of this transformation is continuous auditing and its critical component, continuous control monitoring .

Continuous auditing is a technology-supported approach that allows auditors to evaluate controls, transactions, and risk indicators not at the end of periods, but at or very close to the time the transaction occurs. Li et al. (2024) consider continuous auditing as generating assurance simultaneously with or shortly after the occurrence of the assured events; they state that this approach is based on real-time or frequent auditing, data modeling, and analytical monitoring dimensions. This definition transforms continuous auditing from merely a technical automation tool into a strategic assurance model in terms of

obtaining audit evidence in a timely manner, quickly detecting control deviations, and informing management in a timely manner.

Continuous audit monitoring refers to the continuous monitoring of a business's critical control points using automated tools. This includes the continuous monitoring of access controls, separation of duties, approval limits, transaction matching, abnormal transaction patterns, system configurations, data integrity, and security events. ERP systems, financial transaction platforms, cloud-based applications, and cybersecurity monitoring tools are particularly important data sources for continuous audit monitoring. Farras et al. (2025) state that continuous audit methods work in conjunction with real-time accounting systems; and that transactions and internal controls can be continuously evaluated through automated software, embedded audit modules, and advanced audit tools .

At this point, continuous control monitoring differs significantly from traditional control tests. In traditional auditing, the auditor forms an opinion about the design and effectiveness of the control by examining documents, transaction samples, or control evidence for a selected period. In continuous control monitoring, however, control performance is monitored instantly or periodically through system data. Thus, control deficiencies, errors, and irregularities can be detected not at the end-of-period audit, but at the time they occur or within a short period. This strengthens the corrective effect of the audit and allows management to take timely action.

One of the most important benefits of continuous audit monitoring is that it supports the transition from sample-based auditing to full population testing . While in traditional auditing the auditor usually examines only a specific portion of the transactions, continuous auditing technologies can enable testing the entire transaction universe. Farras et al. (2025) emphasize that continuous auditing can perform bidirectional analysis at the transaction and account balance level, going beyond the traditional sample approach and allowing each transaction to be evaluated . This is a key feature that improves audit quality, especially in high-volume purchasing, payment, collection, payroll, inventory, and user access processes.

Continuous control monitoring also makes risk-based auditing planning dynamic. As control deviations, anomaly alerts, and transaction intensities are regularly monitored, the internal audit unit can see earlier in which processes the risk is increasing. Thus, audit resources can be directed to areas with increasing risk intensity without being tied to fixed annual plans. Omolere (2025) states that continuous auditing can identify suspicious behaviors and control failures at an early stage by monitoring data flows such as system logs , network traffic, user activity, and application operations; this transforms internal audit from a reactive function to a proactive risk management mechanism .

For continuous monitoring to be effective, technological infrastructure alone is insufficient. The correct selection of control points to be monitored, the reasonable setting of alert thresholds, the reliability of data sources, and the linking of alerts to the responsibility matrix are necessary. Otherwise, the system will generate a large number of false positive alerts and create an information overload for auditors. Farras et al. (2025) state that information overload is a significant risk in continuous monitoring systems, that too many alerts can make it difficult for auditors to identify critical issues, and therefore alert systems should be prioritized according to their importance .

Therefore, the basic design principles for continuous monitoring systems can be summarized as follows:

Design Element	**Explanation**
Identifying critical control points.	Selection of process, operation and system controls that pose a high risk to the company.
Data source reliability	ERP, CRM, log , banking, payment, payroll, and security systems.
Threshold and rule design	Establishing clear rules for situations such as abnormal operations, unauthorized access, exceeding limits, and violations of separation of duties.

Automatic warning mechanism	When a deviation occurs, notification is sent to the auditor, process owner, or risk unit.
Escalation process	Referral of critical findings to management, audit committee, or information security teams.
Monitoring and improvement cycle	Updating the control design, process flow, and audit plan based on the warning results.

Continuous control monitoring, particularly in the context of internal audit, is not merely a mechanism for detecting errors, but also an early warning system that measures the quality of the control environment. Through these systems, auditors can monitor the control performance of process owners, assess the continuity of management controls, and provide the audit committee with more up-to-date assurance information. However, the independence aspect of this approach must be carefully managed. Farras et al. (2025) state that excessive intertwining of continuous control tools with management performance monitoring systems can create risks for auditor independence . Therefore, the role of internal audit should not be to operate the control, but to provide independent assurance about the design and operational effectiveness of the control.

12.2. Real-Time Audit Systems

Real-time monitoring systems are systems that enable the analysis of data generated from business operations in real-time or with very short delays. These systems can monitor not only financial transactions but also operational processes, cybersecurity incidents, user behavior, system performance, and control effectiveness. Thus, the monitoring function becomes structured in a way that allows for intervention at the moment a risk arises, rather than focusing solely on retrospective error detection.

Real-time audit systems are generally built on an integrated architecture that connects data collection, analytical processing, and assurance reporting. At the data collection stage, information is drawn from multiple internal and external sources, including ERP transaction records, bank movements, payroll data, purchase orders, invoices, user logs, network activity, system configurations, and externally obtained datasets. This information is then processed through analytical mechanisms such as rule-based tests, exception analysis, statistical anomaly detection, machine learning models, and cross-validation procedures. The outputs generated from these analyses are transformed into dashboards, automated alerts, and exception reports that can be used by auditors, management, and the audit committee. Omolere (2025) explains continuous audit architecture through the interaction of data, analytics, and reporting components, emphasizing that such a structure enables real-time evaluation of sources such as system logs, user activity, and network data, particularly in cybersecurity audits.

The most critical element in real-time audit systems is the ability to cross-verify audit evidence not only from internal accounting records but also from different sources. Li et al. (2024) propose the real-time processing of textual audit evidence and its cross-verification with accounting data within a continuous audit framework supported by large language models. The three-stage model developed in the study consists of the following steps: pre-processing of the text, LLM inference guided by auditor objectives and diagrams, and verification of the audit evidence obtained from the LLM with accounting records . This approach expands the scope of real-time auditing, particularly in public procurement, payroll, contract auditing, personnel transactions, and the control of externally sourced documents.

Li et al. (2024), applied to a public payroll system in Brazil, demonstrates the practical benefit of real-time audit systems. The model cross-validated payroll records with human resources information published in the Official Gazette , enabled full population testing compared to the existing manual process, reduced cross-validation time by 83%, and achieved 96% accuracy in the separated audit evidence. This finding shows that real-time audit systems not only

provide speed but also improve assurance quality by expanding audit coverage.

Another important application area for real-time monitoring systems is cybersecurity. Since cyber incidents can escalate within minutes, a periodic monitoring approach may be insufficient to detect these risks in a timely manner. Omolere (2025) states that real-time monitoring is a process of continuously collecting, analyzing, and reporting system and network activities; this approach can quickly detect unauthorized access, data leakage, unusual network traffic, and control failures . In this context, SIEM systems, endpoint detection and Response tools, network traffic analysis, and user behavior analytics are among the core technologies of real-time monitoring systems.

The main technologies used in real-time monitoring systems can be summarized as follows:

Technology	**Control Function**
ERP embedded control modules	Monitoring violations of transaction rules, approval limits, and separation of duties.
RPA	Automation of repetitive tasks such as data retrieval, reconciliation, reporting, and control testing.
Artificial intelligence and machine learning	Anomaly detection, risk scoring , predictive analysis, and pattern recognition.
Big data analytics	Analyzing high volumes of structured and unstructured data.
SIEM / EDR / UEBA	Monitoring cybersecurity incidents, user behavior, and system activity.
Text analytics supported by LLM	Separation of contracts, minutes, official documents, announcements, and textual evidence for audit purposes.
Cloud-based monitoring platforms	Centralized analysis of data from distributed systems.
Dashboard and visualization tools	Presenting findings, exceptions, and risk indicators to management.

Artificial intelligence and machine learning enhance the analytical capacity of real-time audit systems. Al-Omush et al. (2025) state that artificial intelligence can process large datasets in financial auditing to

detect anomalies, patterns, and potential fraud indicators; thus, overcoming the limitations of traditional sampling methods and enabling auditors to examine the entire transaction universe. However, the "black box" nature of artificial intelligence systems creates new risks in terms of explainability , data quality, ethical responsibility, and auditor judgment. Therefore, real-time audit systems should be designed not only with automation logic but also with governance and assurance logic.

Another issue to consider when establishing real-time audit systems is false positives and false negatives. Overly precise rules can generate an unnecessary number of alerts; overly broad thresholds can lead to significant risks being overlooked. Li et al. (2024) state that while high accuracy is achieved in LLM-supported continuous auditing, false positives and false negatives are not completely eliminated, and therefore the model needs to be improved through fine-tuning, human evaluation, and process feedback . This does not diminish the importance of the human auditor in real-time auditing; rather, it transforms the auditor's role into data interpretation, exception evaluation, and assurance decision-making.

12.3. Smart Dashboards

Intelligent dashboards are a critical tool for making the data obtained from continuous auditing manageable. Real-time audit systems generate large amounts of data; however, unless thi s data is transformed into meaningful indicators, its decision value remains limited for auditors and management. Intelligent dashboards make audit information manageable and traceable by visually presenting transaction exceptions, control deviations, risk scores, anomaly alerts, audit findings, and action statuses.

The primary function of intelligent dashboards is not just reporting. These dashboards provide early warning, risk prioritization , finding tracking, root cause analysis, performance measurement, and management decision support in audit processes. Omolere (2025) states that real-time monitoring and continuous auditing complement each

other; monitoring systems provide a continuous flow of data, while continuous auditing frameworks define rules, thresholds, and procedures for evaluating this data. In this integration, automated alerts, anomaly analysis, reporting, and improvement processes are key components.

A smart control dashboard are:

Display Area	**Example Metrics**
Control activity	Success/failure control tests, control deviation rate, repeated control violations
Process anomalies	Unusual amounts, duplicate payments, unauthorized changes, exceeding limits
Access controls	Unauthorized access attempts, violations of separation of duties, privileged user activities.
Financial process risks	High risk in purchasing, payment, collection, inventory, and payroll processes.
Cybersecurity indicators	Suspicious login , data transfer, abnormal network traffic, system configuration changes.
Audit actions	Number of open cases, delayed actions, completed corrective actions
Management reporting	Summary risk outlook, trend analysis, and high-priority findings for the audit committee.

One of the main advantages of intelligent dashboards is that they help auditors quickly identify critical risks within high-volume data. Farras et al. (2025) emphasize that auditors working with big data may experience difficulties with information overload, pattern detection, and unstructured data interpretation . Therefore, simple, prioritized , and action-oriented presentations should be preferred in dashboard design . If every alert is presented at the same level of importance, the decision support value of the system decreases. Therefore, alerts should be categorized into critical, high, medium, and low risk categories; and an automated escalation process should be defined for critical alerts.

Intelligent dashboards should generate information at different levels, not only for internal auditors but also for management, risk management, compliance, information security, and the audit committee.

While internal auditors perform detailed analysis at the transaction and evidence level, senior management is interested in more concise risk scores, trends, and action statuses. The audit committee, on the other hand, wants to monitor the overall state of the control environment, critical findings, recurring weaknesses, and management's corrective action performance. Therefore, the dashboard architecture should be multi-level.

Smart dashboards are becoming increasingly critical, especially in AI-powered audit models. Muhammad et al. (2026) propose that in the Audit -as- Code approach, audit and assurance processes are transformed from written policy documents into machine-verifiable evidence packages; they state that the system can generate PASS/ WARN/ BLOCK decisions, traceability, explainability , and risk scores . In this approach, the dashboard is not just a results screen; it is also an assurance interface that explains which control passed and why, which deficiency caused a warning, and under what circumstances a blocking decision was generated .

Smart dashboard design should consider the following principles:

1. **Risk-focused approach:** Findings with the highest impact and probability should be presented first.
2. **Traceability:** Each indicator must be linked to the process, control, data source, and audit evidence upon which it is based.
3. **Explainability :** The reasoning behind the scores generated by the artificial intelligence or analytical model must be understandable.
4. **Action link:** Each finding should be associated with a responsible person, a target date, and a corrective action.
5. **Real-time:** Data in critical controls must be updated instantly or at short intervals.
6. **Authorization:** Each user should only be able to view data appropriate to their role.

7. **Independence:** The dashboard must maintain a boundary between a management monitoring tool and an internal audit assurance tool.

These principles ensure that dashboards are not only a visual reporting tool but also an assurance platform that links audit evidence, control performance, and management actions.

Cloud-based systems also enhance the use of intelligent dashboards . Muthusamy (2024) states that in banking project environments, cloud-based AI metric models increase real-time monitoring, operational transparency, and quality assurance; and support reliability in distributed operations through continuous data acquisition, intelligent metric calculation, and adaptive alert mechanisms . This approach makes it possible to monitor risk and control data from different systems through centralized dashboards , especially in large-scale financial institutions .

12.4. Integrated Assurance Models

Continuous monitoring and real-time assurance are not limited solely to the use of technology in the internal audit function. This approach requires integrated operation with the organization's risk management, internal control, compliance, information security, data governance, AI governance, and management oversight functions. Therefore, integrated assurance models are becoming increasingly important in the modern audit approach.

Integrated assurance represents a coordinated governance mechanism that brings together different assurance activities around a common understanding of organizational risk. Rather than treating risk management, compliance, information security, internal control, and internal audit as isolated functions, this approach seeks to align their roles, responsibilities, and reporting practices. Operational management remains responsible for establishing and operating controls within daily business activities, while specialist oversight functions support the organization through monitoring, policy guidance, and

risk-related expertise. Internal audit contributes to this structure by independently evaluating whether governance, risk management, and control processes are appropriately designed, effectively implemented, and capable of supporting reliable organizational oversight.

Continuous audit systems can strengthen integrated assurance by consolidating and analyzing data generated across these three lines. Through such integration, assurance activities can move beyond fragmented and periodic reviews toward a more dynamic, timely, and evidence-based structure. This enables organizations to identify emerging risks earlier, reduce duplication among assurance functions, and provide management and the audit committee with a more comprehensive view of the control environment.

Nandal (2026) proposes a three-layered framework for AI-assisted audit assurance: a predictive intelligence layer, a governance control layer, and an audit assurance layer. In this model, AI systems are treated not merely as tools that generate risk scores or anomaly alerts, but as governance objects that need to be audited . This approach suggests that continuous assurance models will not be limited to transaction auditing in the future; algorithms, models, data sources, and automated decisions will also fall under the scope of auditing.

The basic logic of the integrated assurance model can be established as follows:

Layer	**Main Objective**	**Examples of Activities**
Predictive intelligence	Generating a risk signal	Anomaly detection, risk scoring, classification, prediction.
Governance controls	To ensure model and system reliability.	Model validation , explainability , bias testing, fit check.
Audit assurance	To conduct an independent evaluation.	Control test, model verification, continuous monitoring, assurance report.

Management and committee oversight	Monitoring risk decisions.	Dashboard, action tracking, policy updates, risk appetite assessment.

Nandal (2026) states that the AI audit governance layer should include model validation, explainability checks, bias and fairness tests, compliance monitoring, and monitoring protocols. In this context, assurance does not depend solely on whether the AI model has a high accuracy rate. How the model works, what data it is fed with, how its decisions can be explained, what controls it is monitored with, and in what situations human intervention is needed are also within the scope of assurance.

In integrated assurance models, continuous auditing performs both a monitoring and an assurance-enhancing function. On the one hand, it enables the ongoing examination of financial and operational processes by supporting continuous control assessment, exception detection, and risk monitoring. On the other hand, it creates an additional assurance need regarding the digital tools used within the audit process itself, particularly artificial intelligence, data analytics, and automation systems.

This second dimension is especially important in AI-enabled audit environments. When internal audit relies on predictive models, automated analytics, or algorithmic decision-support tools, the reliability of audit conclusions depends not only on the underlying business data but also on the design, governance, transparency, and validation of these technological systems. If such tools produce inaccurate, biased, or unexplained outputs, they may weaken rather than strengthen audit assurance. Therefore, continuous auditing should also include mechanisms for evaluating whether AI-based audit tools operate within appropriate governance, validation, and accountability structures.

Nandal (2026) emphasizes that the efficiency gains produced by predictive models are not sufficient, by themselves, to ensure reliable auditing or assurance in the absence of governance controls. From this perspective, AI-enabled audit systems should be designed as auditable

control systems with embedded governance mechanisms. Such systems can support continuous assurance only when their outputs are traceable, explainable, monitored, and subject to periodic validation.

The integrated assurance model should be able to answer the following control and assurance questions:

Question of Assurance	**Importance from an Audit Perspective**
Which risks are being monitored in real time?	This indicates whether the audit scope is risk-focused.
Which controls are being tested automatically?	Continuous monitoring defines the scope of the monitoring.
How are alert thresholds determined?	It affects the risk of false positives and false negatives.
How are artificial intelligence models validated?	This is necessary for model reliability and auditability.
Where does the dashboard data come from?	This is important for data integrity and evidence reliability.
To whom are the findings reported and when?	It demonstrates escalation and governance effectiveness.
How are corrective actions monitored?	It supports a continuous improvement cycle.
How is the independence of internal audits protected?	It ensures the objectivity of the assurance function.

Continuous auditing and integrated assurance models also provide significant benefits in the field of cybersecurity. Omolere (2025) states that continuous auditing provides timely information about cyber risks and control performance to senior management and audit committees through real-time dashboards , automated alerts, and periodic reports; this strengthens governance and compliance processes . This structure contributes to the continuous monitoring of control compliance, especially within frameworks such as ISO 27001, NIST, GDPR, KVKK, and SOX.

However, certain risks should not be overlooked when implementing integrated assurance models. Data quality issues, lack of system integration, technical skill gaps in audit teams, model explainability ,

algorithmic bias, over-reliance on automation results, and blurring of independence boundaries are among the main risks. Omolere (2025) states that continuous auditing involves challenges such as data quality, system integration, skill gaps, and governance of automated audit processes; and that the use of advanced analytics and artificial intelligence creates risks such as model transparency, false positives, and over-reliance on automated outputs by the auditor .

Therefore, in an integrated assurance model, the human auditor should not be excluded from the system. On the contrary, the auditor should be positioned as an independent assurance actor who evaluates model results, questions the quality of evidence, prioritizes warnings , interprets control deficiencies, and monitors management actions. Artificial intelligence and automation should be considered not as replacements for the auditor, but as tools that enhance the auditor's scope and analytical power.

Chapter Summary

Continuous monitoring and real-time assurance are among the key approaches shaping the future of internal audit functions in digital businesses. This model transforms auditing from a periodic and retrospective review into a continuous, data-driven, risk-based, and technology-supported assurance mechanism. When continuous control monitoring, real-time audit systems, intelligent dashboards , and integrated assurance models are considered together, it is evident that the internal audit function is elevated to a more proactive , strategic, and decision-supporting position within the company.

However, continuous monitoring doesn't simply mean using more technology. An effective continuous monitoring model requires proper control design, reliable data architecture, explainable analytical models, qualified audit teams, the principle of independence, governance mechanisms, and robust reporting processes. Otherwise, systems can become mere technical tools that generate numerous warnings but offer limited assurance value.

The resources discussed in this section demonstrate that continuous auditing expands the scope of operations, enables real-time risk detection, and allows for faster processing of audit evidence with AI and LLM-supported models; however, these technologies must necessarily be supported by governance and assurance controls. Therefore, continuous auditing and real-time assurance are not merely technical innovations in modern internal auditing; they represent a redesign of audit methodology, control understanding, and organizational assurance architecture.

Chapter 13 – Future Competencies of Internal Auditors

Introduction

Digital transformation has fundamentally changed the scope and nature of the internal audit function. Traditionally seen as limited to reviewing past transactions, checking documents, and ensuring regulatory compliance, internal audit has now become a strategic function closely linked to areas such as data analytics, artificial intelligence, cybersecurity, automation, digital governance, and ethical technology use. This transformation has also significantly broadened the competency set expected of internal auditors.

Today's internal auditors must not only possess knowledge of accounting, control, and regulations; they must also be able to understand data, interpret digital systems, assess technological risks, question the ethical dimensions of algorithmic decision-making processes, and communicate their findings clearly and effectively to different stakeholders. Therefore, in the digital age, internal audit is no longer merely a control activity that detects errors or nonconformities; it is transforming into a consulting and assurance mechanism that supports decision-making processes, anticipates risks, provides digital assurance, and strengthens corporate resilience.

In this context, the internal auditor of the future should be viewed not merely as a "controlling" professional, but as someone who gives meaning to data, questions the risks of technological systems, communicates with management at a strategic level, possesses high ethical sensitivity, and is open to continuous learning. The effectiveness of the internal audit profession in the digital age depends on the combined development of technical knowledge with analytical thinking, ethical reasoning, communication skills, and digital literacy.

This section addresses five key competency areas that stand out for future internal auditors: data literacy, technology skills, analytical

thinking, ethical awareness, and communication in digital environments.

13.1. Data Literacy

Data literacy is the capacity of an internal auditor to read, interpret, and question data not merely as a numerical output, but as audit evidence, risk indicators, and decision support elements. In digitized businesses, transaction volumes have increased significantly; financial and operational processes are now conducted through ERP systems, cloud-based applications, customer relationship management systems, digital payment infrastructures, and automated reporting tools. This situation renders it insufficient for internal auditors to remain limited to traditional sampling approaches.

Ahmed and Japee , advanced data analytics enables internal auditors to test on full datasets instead of selected samples, perform real-time monitoring, and improve the accuracy, reliability, and timeliness of audit results through anomaly detection (Ahmed & Japee , 2025). At this point, data literacy is becoming not just a technical skill, but a fundamental professional competency that directly affects the quality of auditing.

A data-literate internal auditor will first and foremost question the source, integrity, accuracy, and reliability of the data. For example, in a sales revenue audit, simply reviewing accounting records is insufficient. The internal auditor must assess data consistency across the sales order system, billing system, collection records, customer database, return records, and inventory movements. Such cross-data checks facilitate the detection of revenue manipulation, fraudulent invoicing, period shifting, unauthorized transactions, and unusual transaction patterns.

Mat Ridzuan et al. state that digital technology skills play a critical role, particularly in fraud risk assessment; data visualization, data extraction, and analytical skills are among the essential digital competencies for auditors (Mat Ridzuan et al., 2022). The study also notes that fraudulent transactions can be hidden within company databases,

therefore auditors lacking sufficient digital technology skills may have difficulty detecting fraud risks.

Data literacy also requires the auditor to be able to recognize data quality issues. Missing data, duplicate records, misclassified transactions, inconsistent date formats, manual interventions, off-system records, and unauthorized data modifications can directly affect the audit result. Therefore, the internal auditor should not blindly trust the data; they should analyze how the data was generated, who may have modified it, what controls it underwent, and which systems it was fed from.

Another dimension of data literacy is visualization competence. Internal auditors are no longer limited to preparing long text reports; they are producing risk boards, charts, heat maps, and dashboards for the board, audit committee, and senior management. This makes complex transaction sets more understandable and enables decision-makers to grasp risks more quickly. Ahmed and Japee's study highlights how data analytics improves the quality of decision-making in internal audit through full population testing and anomaly detection.

For the internal auditor of the future, data literacy should encompass the following sub-skills:

- Identifying data sources and monitoring data flows,
- Testing data integrity and accuracy,
- Performing anomaly and exception analyses,
- Using basic data visualization tools,
- ERP interprets data relationships between accounting, inventory, sales, and payment systems.
- Transforming data analytics results into audit evidence.
- Being aware of data privacy and security issues.

In this context, data literacy not only enhances the internal auditor's technical capacity but also broadens the scope of the audit, improves the quality of findings, and contributes to earlier risk detection. In the digital age, an internal auditor who is not data literate can only see the

true risk profile of the company in a limited and fragmented way. In contrast, a data literate internal auditor can establish relationships between scattered data, generating more meaningful, predictive, and strategic insights for management.

13.2. Technology Skills

Technological skills refer to an internal auditor's ability to understand digital systems, automation tools, artificial intelligence applications, cybersecurity controls, ERP structures, cloud technologies, and data analytics platforms from an audit perspective. Digital transformation does not require internal auditors to be technology experts; however, it does necessitate developing a level of technical awareness that enables them to understand how technological systems work, what risks they generate, and what controls should be used to manage them.

According to Usul and Alpay, artificial intelligence, blockchain , robotic process automation, and data analytics are transforming internal audit paradigms, providing capabilities such as real-time transaction analysis, continuous monitoring, and anomaly detection (Usul & Alpay, 2025). However, the same study emphasizes that these technologies also bring new risks such as cybersecurity threats, algorithmic bias, data privacy breaches, and a lack of expertise.

In this context, the technological competence of internal auditors should be understood as a multidimensional capability rather than as a single technical skill. At a basic operational level, internal auditors are expected to use digital tools that support audit execution, documentation, analysis, and reporting. These tools may include data analytics software, electronic working papers, audit management systems, reporting platforms, dashboard applications, and basic query tools. Such competencies enable auditors to work more efficiently with digital evidence and to conduct audit procedures in a more systematic and data-driven manner.

Beyond the use of technology, internal auditors should also be capable of evaluating the control environment surrounding technological systems. This requires knowledge of access rights, user roles, system-

based controls, change management procedures, log records, data backup processes, disaster recovery arrangements, and cybersecurity controls. In this respect, technology is not only a tool used by the auditor, but also an audit object that must be assessed in terms of reliability, security, continuity, and control effectiveness.

At a more strategic level, internal auditors are increasingly expected to interpret the broader risks created by digital transformation. This includes assessing how artificial intelligence models influence decision-making processes, how algorithmic bias may affect organizational outcomes, how automation changes the control environment, and how digital dependency may shape organizational resilience. Therefore, the internal auditor's technological competence should combine practical tool usage, information systems assurance, and strategic risk interpretation. Such an integrated competence profile is essential for internal audit functions that aim to provide meaningful assurance in digitally transformed organizations.

Djogo's work indicates that in the age of digital disruption, internal auditors need to keep up with technological advancements such as cloud technology, artificial intelligence, and big data analytics; and that internal auditing is becoming more critical in maintaining internal controls and regulatory compliance in virtualized business processes (Djogo , 2023). This finding demonstrates that internal auditors should approach technology not as an external element, but as an integral component of the audit universe.

A crucial aspect of technology skills is cybersecurity awareness. As digitalization increases, organizations increasingly store financial, operational, and personal data in digital environments; this increases threats such as unauthorized access, data leakage, ransomware attacks, third-party service provider risks, and system disruption. Ahmed and Japee's systematic review reveals that cybersecurity has now become a central responsibility of internal audit; auditors need to assess cyber governance frameworks, resilience strategies, and digital risk controls.

Technological skills also require the internal auditor to maintain professional skepticism regarding automation. Artificial intelligence and

automation systems can speed up the audit process; however, the results produced by these systems need to be critically evaluated by the auditor. Usul and Alpay state that over-reliance on technology can weaken professional skepticism and that unquestioning trust in algorithmic outputs can create risks (Usul & Alpay, 2025). Therefore, the internal auditor of the future should be a professional who uses technology but doesn't think for technology.

Key areas that internal auditors need to develop in terms of technology skills include:

- Understanding the operation and control points of ERP systems,
- Ability to use data analytics and visualization tools,
- Evaluating the auditing impacts of artificial intelligence and automation applications.
- Ability to test cybersecurity and data privacy controls,
- Assessing the risks of cloud systems and third-party service providers.
- Analyzing log records, user permissions, and system changes,
- Interpreting technology-related ethical and regulatory risks.

In conclusion, technological skills are indispensable for internal auditors to provide assurance in digital organizations. An internal audit function that does not understand technology risks superficially assessing the most critical risk areas of the company. Conversely, technologically proficient internal auditors can provide management with stronger assurance and advice by holistically addressing both the opportunities and risks of digital processes.

13.3. Analytical Thinking

Analytical thinking is the internal auditor's ability to break down information into its components, see relationships, establish cause-and-effect connections, recognize unusual patterns, and interpret findings

within the broader organizational context. In the digitalized audit environment, internal auditors are faced with significantly more data, system outputs, reports, indicators, and risk signals. Therefore, simply collecting information is not enough; this information needs to be analyzed in a meaningful way.

Djogo states that critical thinking and a broad business perspective are essential competencies for auditors. According to the study, auditors should be able to evaluate evidence, identify hidden patterns or trends, determine potential risk and problem areas, and interpret findings within the macroeconomic, sectoral, and operational conditions of the company (Djogo , 2023).

Analytical thinking is a core competence for internal auditors, particularly in digital audit environments where risks may emerge through complex data flows, automated processes, and system-generated transactions. Unlike traditional audit approaches that often rely on year-end reviews and retrospective examination of records, analytical thinking enables internal auditors to identify risk indicators while processes are still ongoing. Unusual supplier concentrations in payment transactions, payments made by different companies to the same IBAN, user accounts that are frequently opened and closed, or transactions recorded outside normal working hours may all function as early warning signals. In this respect, analytical thinking supports a more proactive audit approach by allowing risks to be detected before they develop into material control failures or financial losses.

Analytical thinking also strengthens the root cause analysis of audit findings. An internal auditor should not limit the evaluation to identifying an error or stating that a control has failed. The more important task is to determine why the error occurred, which process weakness enabled it, whether the issue is linked to a systemic or managerial deficiency, and what type of control design is required to prevent recurrence. This approach expands the role of internal audit beyond the reporting of exceptions. It positions internal audit as a function that contributes to process improvement, control redesign, and risk reduction.

The strategic contribution of internal audit is also closely connected to analytical thinking. In the digital age, internal audit is increasingly expected to support corporate decision-making, value creation, and sustainable governance rather than merely provide financial assurance. Ahmed and Japee (2025) emphasize this broader strategic role of internal audit, while Alsagoor et al. (2024) underline the relevance of digital transformation, emotional intelligence, and organizational culture for internal audit quality. In this context, internal auditors should evaluate findings not only as technical nonconformities, but also in relation to organizational objectives, risk appetite, regulatory compliance, operational performance, and institutional resilience.

Analytical thinking is therefore inseparable from professional skepticism. Digital systems may produce dashboards, reports, alerts, or risk scores, but internal auditors should not accept these outputs without critical evaluation. For example, a dashboard may present all indicators as "green," yet this appearance may be misleading if the underlying data include missing records, incorrect classifications, unauthorized manual interventions, or poorly designed control parameters. An analytically oriented internal auditor examines not only the final output, but also the data generation process, system logic, control mechanisms, and management assumptions behind that output. This enables internal audit to provide assurance that is not merely data-driven, but also judgment-based, evidence-oriented, and strategically relevant.

Rumasukun states that auditor competencies are not limited to technical knowledge; critical thinking, analytical skills, communication, and ethical reasoning also play a fundamental role in the audit process (Rumasukun, 2024). In this context, analytical thinking is not only a cognitive skill for the future internal auditor, but also a competency central to professional reasoning.

In the future, internal auditors are expected to develop the following skills within the scope of analytical thinking:

- Establishing meaningful relationships between complex data sets,
- Identifying unusual trading patterns and risk indicators,

- Perform a root cause analysis.
- Interpreting the findings in operational, financial, and strategic contexts.
- Questioning the reliability of digital system outputs,
- Assessing the organizational impact of control vulnerabilities,
- Reaching a balanced professional judgment by considering alternative explanations.

An internal auditor with well-developed analytical thinking skills not only examines whether existing controls are working; they also anticipate the risks the company may face in the future, identify fragile processes, and predict areas where control design needs strengthening. In this respect, analytical thinking is one of the key determinants of the future strategic value of internal auditing.

13.4. Ethical Awareness

Ethical awareness means that the internal auditor, while conducting their professional activities, adheres to the principles of integrity, impartiality, independence, confidentiality, accountability, and the public interest; and also recognizes the new ethical risks posed by digital technologies. In the digital age, ethics are not limited to adherence to traditional professional rules. New issues such as data privacy, algorithmic bias, transparency of AI decisions, manipulation in automated reporting systems, cybersecurity negligence, and digital exclusion have also fallen within the scope of ethical awareness.

Adriansyah et al. state that in the digital age, accounting professionalism consists of a combination of ethical integrity, technical skills, and digital adaptability. In their study, professionalism is defined not only as technical competence but also as a multidimensional construct shaped by ethics, expertise, and adaptation to technological transformation (Adriansyah et al., 2025). This approach is directly applicable to internal auditing as well. When using digital systems, internal

auditors should not only focus on producing efficient results, but also question whether these results were obtained fairly, reliably, transparently, and responsibly.

It is particularly important to address digital competence as part of an ethical framework. Adriansyah et al. argue that digital competence should be positioned not merely as an additional skill, but as part of a professional ethical framework that includes using technology responsibly, fairly, and inclusively. The same study suggests that ethics, competence, and technology should be viewed as an ecosystem; that unethical but technically proficient professionals can pose a moral hazard, while ethical but digitally incompetent professionals may lose their professional credibility.

Ethical awareness in internal auditing is becoming increasingly critical, particularly with the widespread adoption of artificial intelligence and algorithmic decision-making systems. AI-powered audit tools can make significant contributions in areas such as fraud detection, risk scoring, and anomaly analysis. However, if the datasets used to train these tools are flawed, incomplete, or biased, the results produced by the system may also be incorrect or unfair. Therefore, the internal auditor should evaluate the AI output not merely as a technical result, but as a decision support element with ethical and governance dimensions.

Ahmed and Japee emphasize that ethical and regulatory issues such as data privacy, algorithmic bias, and the responsible use of artificial intelligence in digital audit applications are critical to audit integrity (Ahmed & Japee , 2025). Similarly, Usul and Alpay state that digital transformation places new responsibilities on the internal auditor in the areas of ethical AI governance and cyberresilience (Usul & Alpay, 2025).

Ethical awareness is also related to the internal auditor's ability to maintain independence and impartiality. Digitalization is bringing internal audit closer to management, making its advisory role a stronger function. However, while the advisory role increases, the internal auditor's independent position as a provider of assurance should not weaken. The internal auditor should be able to contribute to digital

transformation projects while independently assessing the risks of these projects. For example, internal audit can provide consultancy during the installation of an AI-powered credit rating system; however, it must maintain objectivity when subsequently evaluating the control effectiveness of the same system.

Within the scope of ethical awareness, the key areas that a future internal auditor should develop are as follows:

- Data privacy and personal data protection awareness,
- Questioning the risk of bias in artificial intelligence and algorithmic decision systems,
- Evaluating the reliability and integrity of digital evidence.
- Upholding the principle of independence and impartiality in digital consulting roles,
- Understanding the ethical and organizational consequences of cybersecurity negligence,
- Ensuring transparency, accountability, and fairness in the use of technology,
- Maintain professional skepticism even in the face of automated system outputs.

Ethical awareness in the digital age transforms the internal auditor from a mere technical user into an assurance professional who questions the organizational, human, and societal consequences of technology. Therefore, in the future, the credibility of internal auditing will depend not only on the power of the technology used but also on the ethical judgment of the auditor using that technology.

13.5. Communication in Digital Environments

Communication competence is the ability of an internal auditor to convey findings, risk analyses, data visualizations, and recommendations clearly, persuasively, and in a stakeholder-focused manner through physical or digital meetings, online platforms, dashboards,

electronic reports, and remote work environments. Digitalization has transformed the nature of internal audit communication. Auditors no longer simply submit written reports; they communicate through real-time risk dashboards, short executive summaries, digital working papers, online meetings, and interactive reporting tools.

Djogo's work positions communication skills as one of the most important competencies for internal auditors. The study states that auditors should be able to clearly convey their thoughts, suggestions, and findings; effectively conduct meetings, presentations, interviews, and negotiations; and prepare reports that can be understood by stakeholders with varying levels of knowledge (Djogo , 2023).

Communication in digital environments is not just about sharing technical findings. The internal auditor must be able to explain complex data analyses in business language that management can understand. For example, simply stating that an "outlier was detected" in a data analytics study is not enough. The internal auditor must clearly explain what this means, in which process it creates a risk, what its financial or operational impact is, and what action management should take.

This skill is becoming increasingly important, especially with the widespread use of dashboards and visual reporting tools. Digital audit reports now utilize risk indicators, trend analyses, heat maps, traffic light indicators, and transaction-based exception lists instead of lengthy texts. However, visualization alone does not equate to effective communication. The internal auditor must also explain the analytical reasoning behind the visual output and its implications for management.

Rumasukun emphasizes the importance of communication skills and emotional intelligence within auditor competencies. According to the study, emotional intelligence plays a significant role in auditor-client relationships, managing difficult conversations, balancing expectations, and establishing trust relationships with stakeholders (Rumasukun, 2024). This skill is even more important in digital environments because the risk of misunderstandings is higher in online meetings, email correspondence, and remote monitoring processes.

Another issue that internal auditors should pay attention to in digital communication is the tone of the findings. Audit findings can often be sensitive for process owners. Especially when dealing with control vulnerabilities, unauthorized transactions, data security breaches, or performance deficiencies, the communication language should be constructive, evidence-based, and solution-oriented. Djogo states that emotional intelligence enables auditors to strike a balance between objectivity and sensitivity to stakeholders' emotions (Djogo , 2023).

Digital communication skills should include the following sub-competencies:

- Writing concise, clear, and evidence-based digital reports.
- Explaining data-driven findings in management language,
- Interpreting dashboard and visual analysis results,
- Making effective presentations in online meetings,
- Asking the right questions and actively listening during remote monitoring interviews,
- Communicating sensitive findings in a constructive and professional manner.
- Developing appropriate communication language for different stakeholder groups,
- Complying with privacy and information security rules in digital communication.

Ahmed and Japee's study also states that modern internal auditors should possess not only technical skills but also non-technical skills such as communication, ethical judgment, and compliance (Ahmed & Japee , 2025).. Therefore, communication in digital environments is not a complementary but an essential competency for the internal auditor of the future.

Chapter Summary

Digital transformation is fundamentally changing the internal audit profession. Artificial intelligence, data analytics, automation, blockchain , and cybersecurity applications are making audit processes faster, more comprehensive, and more predictive; however, they are also creating new risks, ethical issues, and skill gaps. Therefore, the internal auditor of the future cannot be satisfied with traditional audit knowledge. They must be able to read data, understand technology, think analytically, question ethical risks, and communicate effectively in digital environments.

The contemporary internal audit function is increasingly positioned as a value-adding assurance and advisory mechanism rather than a unit concerned only with retrospective compliance review. Its contribution now extends to risk oversight, governance effectiveness, strategic decision support, and organizational resilience (Ahmed & Japee, 2025; Rumasukun, 2024; Alsagoor et al., 2024). To sustain this broader role, organizations need to invest continuously in the development of auditors' digital literacy, ethical judgment, technological skills, analytical competence, and communication capacity.

In conclusion, the internal auditor of the future should possess these five essential qualities: data-savvy, tech-savvy, analytical, ethically sound, and effective digital communication skills. These competencies are critical not only for individual professional development but also for organizations' resilience to digital risks, quality of governance, stakeholder trust, and sustainable governance capacity.

Chapter 14 – The Future of AI-Assisted Auditing

Introduction

AI-assisted auditing should not be considered merely a technological innovation in the internal audit profession. This approach represents a structural transformation that redefines the scope, timing, evidence gathering methods, risk assessment approach, and the auditor's professional role. While the traditional understanding of internal auditing largely relies on sampling, periodic reviews, manual document checks, and retrospective evaluations, AI-assisted auditing creates a more comprehensive, faster, and risk-focused assurance structure through technologies such as big data analytics, machine learning, natural language processing, robotic process automation, anomaly detection, continuous monitoring, and predictive analytics.

This section examines how AI technologies are transforming internal audit practices. It first explains the impact of autonomous control systems on audit processes, then evaluates how a predictive risk assessment approach can be used in internal auditing. Finally, it discusses the contributions of AI use to audit activities and the accompanying ethical, managerial, and regulatory risks. In this context, this chapter aims to demonstrate how AI-assisted auditing can transform the internal audit function into a more continuous, analytical, risk-focused, and strategic structure in the future.

The fundamental reason for this transformation is the continuous increase in the quantity, speed, variety, and complexity of data generated in businesses. Financial transactions, ERP records, electronic invoices, bank transactions, payroll data, inventory movements, contracts, emails, access logs, and digital transaction traces significantly expand the potential evidentiary field of internal auditing. This data density creates a structure that is difficult to analyze in all its aspects with classical manual audit methods. In contrast, artificial intelligence systems can detect

recurring patterns, deviations, unusual relationships, and potential risk indicators more quickly within large datasets.

The future of AI-assisted auditing is being shaped by the increasing integration of automation, predictive analytics, and governance-oriented control mechanisms into audit processes. As artificial intelligence tools become more advanced, certain audit procedures may be performed with limited manual intervention. Automated systems can support tasks such as anomaly detection, transaction screening, exception reporting, document review, and continuous control testing. This development moves internal audit away from a purely periodic review model and brings it closer to a continuous monitoring and continuous assurance approach.

Predictive risk assessment is another important direction in the evolution of AI-assisted auditing. By learning from historical transaction data, control exceptions, fraud indicators, and operational patterns, artificial intelligence models can help auditors identify risk signals before they escalate into material problems. This enables internal audit to adopt a more forward-looking role, where the focus is not only on evaluating past transactions but also on anticipating emerging risks and supporting earlier managerial intervention.

At the same time, the growing use of artificial intelligence in auditing creates a stronger need for AI governance and regulatory compliance. AI-enabled audit systems may introduce risks related to data confidentiality, algorithmic bias, explainability, professional responsibility, ethical decision-making, and compliance with legal and regulatory requirements. Therefore, the future of AI-assisted auditing should not be understood merely as the expansion of automation. It should also involve the development of governance structures that ensure AI tools are transparent, auditable, ethically controlled, and aligned with the auditor's professional judgment.

In this context, the future of AI-assisted auditing points not to a model where the auditor is completely eliminated, but to a hybrid audit structure where human auditors and AI systems work together. AI will automate routine and repetitive tasks, allowing the auditor to focus on more complex, analytical areas requiring professional

judgment. Therefore, in the future of internal auditing, AI should be considered not as a replacement for the auditor, but rather as a strategic support mechanism that strengthens audit quality, speed, scope, and risk forecasting.

14.1. Autonomous Control Systems

Autonomous inspection systems are artificial intelligence-powered systems that can perform specific inspection activities without or with limited human intervention. These systems can automatically collect information from data sources, classify operations, monitor checkpoints, detect anomalies, generate risk indicators, and provide early warnings to inspectors. Autonomous inspection systems are based on technologies such as machine learning, robotic process automation, natural language processing, expert systems, artificial neural networks, and process mining (Ali, Abdullah, and Khattab, 2022; Akatak, 2025).

However, the concept of "autonomy" should be used cautiously in the context of auditing. Auditing is not merely a technical data processing activity. It is also a process of assessing the adequacy and appropriateness of evidence, understanding the organizational context, considering ethical risks, questioning management statements, and using professional judgment. Therefore, fully autonomous audit systems may not be sufficient in all cases. Complex financial transactions, management estimates, valuation decisions, indicators of fraud, and ethical dilemmas, in particular, require the assessment of a human auditor (Baharom, 2025; Gökoğlan, Sevim and Kılıç, 2025).

The most significant contribution of AI-powered autonomous systems is the expansion of audit scope. Traditional auditing largely relies on sample selection. The auditor selects specific transactions, tests these transactions, and generalizes the results to the entire universe. However, AI-powered systems can make it possible to analyze the entire transaction universe instead of a sample. Thus, all sales transactions, purchase records, inventory movements, payroll payments, supplier records, system accesses, and accounting vouchers can be examined more comprehensively. This has the potential to improve

audit quality and strengthen anomaly detection (Fırat, 2025; Gökoğlan, Sevim and Kılıç, 2025).

Autonomous audit systems offer significant benefits, particularly in routine, repetitive, and rule-based tasks. Examples include invoice matching, document classification, payment reconciliation, supplier master data checks, payroll compliance tests, authorization conflict analyses, access log review, and the preparation of standard reports. Robotic process automation can accelerate these types of operations, reducing audit time and allowing auditors to focus on higher value-added activities (Ali, Abdullah, and Khattab, 2022; Akatak, 2025).

This transformation also affects the planning, execution, reporting, and monitoring phases of the internal audit function. In the planning phase, artificial intelligence can analyze large datasets to identify high-risk areas. In the execution phase, it can make audit tests more targeted through anomaly detection, pattern recognition, and data mining. In the reporting phase, it can accelerate the classification and presentation of findings to stakeholders. In the monitoring phase, it can automatically track whether the recommended corrective actions have been implemented (Akatak, 2025). Therefore, autonomous systems are shifting internal audit from a periodic control activity to a continuous and data-driven assurance mechanism.

Another contribution of autonomous audit systems is that they strengthen the continuous audit and real-time assurance approach. While traditional audits generally rely on year-end or periodic reviews, AI-powered systems can continuously monitor transactions. Thus, indicators such as abuse of authority, unusual payment behavior, high-risk supplier movements, unusual inventory outflows, or duplicate payments can be identified at an early stage. This structure contributes to the transformation of auditing from a retrospective error-finding function to a real-time risk monitoring function (Fırat, 2025; Wassie and Lakatos, 2024).

However, the success of autonomous audit systems depends on data quality. When AI models are trained with incomplete, erroneous, biased, or inconsistent data, they can produce incorrect results. For example, if certain types of risks have not been sufficiently examined in

past audits, the AI model may also prioritize these risks. Therefore, data integrity, data reliability, data ownership, data security, and data governance become critical in AI-assisted auditing (Baharom, 2025; Wassie and Lakatos, 2024).

Another limitation of autonomous systems is over-reliance on algorithmic outputs. Professional skepticism may weaken if the auditor accepts risk scores or anomaly alerts generated by artificial intelligence without question. Baharom's findings suggest that the use of artificial intelligence can reduce auditors' professional skepticism in some cases, and therefore human judgment should be preserved in AI-assisted auditing (Baharom, 2025). For this reason, autonomous audit systems should be positioned not as ultimate decision-makers, but as analytical systems that support the auditor.

The future of autonomous audit systems is also changing the auditor's job description. The auditor of the future will not be someone who simply checks or reconciles documents. The auditor will become a professional who understands data flow, interprets algorithmic outputs, questions model assumptions, evaluates data quality, tests system controls, and reports technology-related risks to management. Therefore, developing competencies in areas such as data analytics, algorithmic thinking, artificial intelligence literacy, natural language processing, machine learning, robotic process automation, and cybersecurity is becoming essential for auditors (Akatak, 2025; Fırat, 2025).

14.2. Predictive Risk Assessment

Predictive risk assessment is one of the most important areas of development in the future of AI-assisted auditing. While traditional risk assessment is mostly based on past audit findings, financial ratios, management interviews, prior experience, and manual evaluations; AI-assisted predictive risk assessment attempts to predict future risks by analyzing both past and current data. This approach transforms the retrospective control function of internal audit into a prospective risk management function (Fırat, 2025; Gökoğlan, Sevim and Kılıç, 2025).

Artificial intelligence offers significant advantages in risk assessment due to its ability to process large datasets quickly. Machine learning algorithms can learn from past transaction data, identify normal transaction patterns, and mark deviations from these patterns as risk indicators. This helps auditors direct audit resources to riskier areas. According to Fırat, artificial intelligence makes significant contributions to identifying the most critical audit areas, reducing audit risks, and strengthening decision-making processes in risk assessment (Fırat, 2025).

Predictive risk assessment is not based solely on the analysis of financial data. ERP records, system access logs, customer behavior, supplier transactions, contract texts, email content, compliance records, and operational data can also become part of the risk analysis. Natural language processing tools help in the analysis of unstructured data such as contracts, reports, policy texts, and correspondence. In this way, the auditor can perform risk assessment not only with numerical data but also with textual and contextual data (Akatak, 2025; Fırat, 2025).

Predictive risk assessment also makes significant contributions to fraud detection. Fraudulent transactions often leave traces through specific patterns, unusual timings, unauthorized access, duplicate transactions, unrelated supplier movements, unusual payment amounts, or deviations from normal processes. AI-powered systems can detect such complex relationships and unusual patterns more quickly. According to Baharom's review, machine learning applications can provide higher accuracy rates in fraud detection compared to traditional methods; however, this performance can vary depending on the sector, data quality, and application conditions (Baharom, 2025).

What is important at this point is that artificial intelligence is used not only in fraud detection but also in risk prioritization. For example, AI-supported models can provide early warning in areas such as accounts receivable risk, inventory impairment risk, supplier dependency, purchasing irregularities, payroll fraud, cybersecurity vulnerabilities, regulatory non-compliance, and financial reporting errors. Risks can be monitored more dynamically when historical data, transaction frequencies,

amount changes, user behavior, and external indicators are evaluated together (Gökoğlan, Sevim and Kılıç, 2025; Hassan, 2025).

Predictive risk assessment is also transforming audit planning. Traditional internal audit plans are often prepared annually and updated only to a limited extent during the year. However, AI-powered systems can continuously monitor risk indicators, allowing the audit plan to be more flexible and up-to-date. Processes, units, or transaction types with increasing risk levels can be automatically prioritized in the audit plan. This allows the internal audit function to respond more quickly to the changing risk environment (Akatak, 2025; Wassie and Lakatos, 2024).

AI-powered predictive risk assessment has the potential to improve audit quality. These systems can uncover complex relationships and anomalies that a human auditor might not notice within a limited timeframe. Furthermore, analyzing the entire transaction universe can reduce sampling risk. However, improved audit quality cannot be guaranteed solely by using technology. The auditor should support the results generated by the AI system with appropriate audit evidence, understand the assumptions underlying the model, and interpret the results within the organizational context (Baharom, 2025; Fırat, 2025).

One of the significant limitations of predictive risk assessment is algorithmic bias. Since AI models are trained on historical data, they can reproduce past erroneous assumptions or audit deficiencies. For example, if certain departments, transaction types, or risk areas are not adequately represented in historical datasets, the model may underestimate the risks in those areas. Similarly, types of fraud that went undetected in the past may not be learned by the model. Therefore, model validation, data representation, and explainability are essential considerations in AI-assisted risk assessment (Baharom, 2025; Fırat, 2025).

Another limitation is that although artificial intelligence systems produce technical results, translating these results into auditable findings requires human judgment. For example, the system may flag a supplier payment as unusual; however, it is the auditor's responsibility to assess

whether this is an error, fraud, a system record problem, or a legitimate business transaction. Therefore, in predictive risk assessment, artificial intelligence generates a risk signal; but professional analysis is required for this signal to be transformed into an audit finding (Gökoğlan, Sevim and Kılıç, 2025; Baharom, 2025).

Predictive risk assessment also strengthens the role of internal audit within corporate governance. Internal audit is no longer merely a function that reports what happened in the past, but is becoming an assurance and advisory function that provides management with early warning about what might happen in the future. However, this advisory role should not compromise the independence of internal audit. The auditor can provide risk insights to management; however, they should not assume responsibility for management's decision-making (Hassan, 2025; Akatak, 2025).

In this context, the future of predictive risk assessment depends on three conditions: a reliable data infrastructure, a competent auditor profile, and strong AI governance. If data quality is poor, the risk scores generated by the model may be misleading. If the auditor lacks AI literacy, they may not be able to accurately evaluate the system output. If AI governance is weak within the organization, the ethical, legal, and operational risks of the model may not be manageable. Therefore, predictive risk assessment should be considered not merely a technical analysis tool, but a holistic audit transformation (Fırat, 2025; Baharom, 2025; Wassie and Lakatos, 2024).

14.3. Artificial Intelligence Governance and Regulation

One of the most critical issues in the future of AI-assisted auditing is the need for AI governance and regulation. While AI systems provide speed, scope, accuracy, and efficiency in audit processes, they can create new risks when used uncontrollably. These risks include data privacy breaches, algorithmic bias, erroneous model outputs, excessive reliance on automation, unexplained decisions, cybersecurity vulnerabilities, professional accountability ambiguity, and ethical issues (Fırat, 2025; Baharom, 2025; Gökoğlan, Sevim and Kılıç, 2025).

AI governance is a set of rules that defines how AI systems within an organization should be designed, used, monitored, fed with data sources, their outputs verified, and who is responsible for erroneous results. In the context of oversight, AI governance should include topics such as data governance, model governance, ethical principles, explainability, accountability, cybersecurity, human oversight, and regulatory compliance (Wassie and Lakatos, 2024; Baharom, 2025).

Data privacy and security are of fundamental importance in AI-assisted auditing. Internal audit activities often involve sensitive data such as personal data, employee information, customer records, financial information, contracts, trade secrets, and system logs. When AI systems process this data, risks such as unauthorized access, data leakage, misuse of data, and privacy breaches may arise. Therefore, in AI-assisted auditing applications, data access permissions, data retention periods, anonymization, encryption, and data usage limits must be clearly defined (Fırat, 2025; Gökoğlan, Sevim and Kılıç, 2025).

Algorithmic explainability is also central to AI governance. The auditor should be able to understand why the AI system flagged a particular transaction as risky, which variables it considered, and what logic it used to produce its conclusion. Unexplained "black box" systems can call into question the reliability of audit evidence and the professional responsibility of the auditor. In auditing, it is not enough to simply reach a conclusion; the methodology used to reach that conclusion must also be understandable and documentable (Baharom, 2025; Fırat, 2025).

Model validation and performance monitoring are also necessary within the scope of AI governance. An AI model may produce successful results when first established; however, data structures, transaction types, legislation, fraud methods, and business processes may change over time. In this case, the accuracy of the model may decrease. Therefore, AI-powered audit systems should be regularly tested, updated, and monitored for performance. False positive and false negative results of the model should be analyzed, and the accuracy of risk classifications should be reviewed at regular intervals (Wassie and Lakatos, 2024; Baharom, 2025).

Ethical issues in AI-assisted auditing also require special attention. Algorithms can reproduce biases in past data or disproportionately portray certain employees, suppliers, customers, or departments as risky. This can create problems in terms of both fairness and corporate trust. Furthermore, ethical sensitivity increases even more when AI outputs are used in disciplinary, performance, or investigative processes regarding employees. Therefore, AI systems should be used within the framework of impartiality, fairness, accountability, and human oversight principles (Fırat, 2025; Baharom, 2025).

The need for regulation is becoming more visible with the increasing prevalence of AI-assisted auditing. Current auditing standards largely rely on traditional principles of audit evidence, sampling, document review, professional judgment, and audit documentation. However, AI-assisted auditing introduces new types of evidence such as algorithmic risk scores, automated anomaly reports, continuous monitoring outputs, and findings from machine learning models. Clear standards are needed to determine how these new types of evidence should be evaluated, documented, and under what conditions they should be considered sufficient audit evidence (Ali et al., 2022; ,Gökoğlan, Sevim and Kılıç, 2025; Fırat, 2025).

AI governance creates a dual responsibility for internal audit functions. Internal audit should first ensure that the artificial intelligence tools used in its own audit activities are reliable, ethically appropriate, explainable, and subject to performance monitoring. This requires the evaluation of data quality, model accuracy, access controls, validation procedures, bias risks, documentation standards, and the extent to which AI-generated outputs remain subject to professional judgment.

At the same time, internal audit should also expand its audit universe to include artificial intelligence systems used across the organization. AI applications are increasingly embedded in business processes such as credit assessment, recruitment, pricing, customer segmentation, supplier selection, inventory management, fraud detection, and cybersecurity monitoring. These systems may influence operational decisions, stakeholder outcomes, compliance obligations, and risk exposure. Therefore, internal audit should assess whether organizational

AI systems are governed through appropriate policies, accountability mechanisms, ethical safeguards, data protection controls, and monitoring procedures (Akatak, 2025; Baharom, 2025).

At this point, one of the important future tasks of internal audit will be "auditing artificial intelligence." Internal audit will not only be a function that uses artificial intelligence; it will also become an assurance function that evaluates whether the artificial intelligence systems used within the organization operate fairly, reliably, explainably, securely, and in compliance with regulations. This indicates increases the strategic importance of internal audit within corporate governance (Akatak, 2025; Wassie and Lakatos, 2024).

Organizations need to develop written policies and procedures for AI governance. These policies should cover the processes of acquiring, developing, testing, using, monitoring, updating, and decommissioning AI systems. Furthermore, model ownership, data ownership, access rights, ethical review processes, performance monitoring responsibilities, and reporting mechanisms should be clearly defined. Internal audit can assess the adequacy of this structure, providing assurance to the board of directors, audit committee, and senior management (Fırat, 2025; Baharom, 2025).

In the future of AI-assisted auditing, collaboration between regulatory bodies, professional organizations, and businesses will also gain importance. While adapting to technological transformation, the auditing profession must maintain the principles of reliability, independence, impartiality, and professional skepticism. AI systems can speed up auditing; however, audit reliability is determined not only by speed but also by ethics, transparency, accountability, and professional quality (Fırat, 2025; Baharom, 2025).

Chapter Summary

The integration of artificial intelligence into internal auditing is redefining both the operational scope and the professional boundaries of the audit function. By automating repetitive audit procedures,

autonomous systems expand audit coverage and strengthen the shift from periodic review toward continuous assurance. Predictive analytics further changes the role of internal audit by enabling a more anticipatory approach to risk identification, rather than limiting audit work to the examination of historical transactions. However, this transformation also requires a stronger governance framework for AI use, since issues such as ethical responsibility, regulatory compliance, algorithmic explainability, data protection, and professional judgment increasingly shape the responsibilities of auditors in digital audit environments.

This transformation does not diminish the importance of the auditor. On the contrary, it moves the auditor's role to a more analytical, strategic, and technology-oriented position. The internal auditor of the future must be a professional who can leverage data analytics, question the accuracy and reliability of AI outputs, recognize the risk of algorithmic bias, evaluate system controls, and maintain ethical judgment.

In conclusion, the future of AI-assisted auditing does not lie in a fully automated and unmanned audit model; This points to a hybrid assurance model where human auditors and artificial intelligence systems work together. In this model, artificial intelligence will be used as a powerful tool in areas such as data analysis, anomaly detection, risk scoring, and process automation, while the auditor will continue to assume responsibility for professional judgment, ethical evaluation, contextual interpretation, and ultimate assurance. To the extent that this balance is achieved, AI-assisted auditing will improve the quality of internal auditing and strengthen its strategic value within corporate governance.

Conclusion

This book examines the transformation of internal audit in the digital age from theoretical, technological, and applied perspectives. The book's central premise is that internal audit can no longer be viewed as a traditional function that merely checks past transactions, identifies errors and irregularities, or assesses regulatory compliance. Digitalization has fundamentally changed businesses' processes, data production methods, control mechanisms, risk maps, and audit evidence. This transformation has shifted internal audit towards a more strategic, data-driven, technology-supported, risk-based, and continuously assuring structure.

The central finding presented throughout the book is that in the digital age, internal audit has become a central assurance function concerning not only the audit activity itself, but the entire control and governance architecture of the company. Internal audit is no longer limited to examining the accuracy of accounting records or compliance with procedures. The internal auditor must evaluate ERP systems, automated controls, user authorizations, cybersecurity policies, data privacy, AI-powered decision-making mechanisms, continuous monitoring tools, and the reliability of digital evidence. Therefore, modern internal audit is located at the intersection of financial audit, operational audit, information systems audit, fraud audit, ethical assessment, and strategic risk consulting.

The initial chapters of the book examine the fundamental concepts of internal auditing and situate the internal audit function within the broader framework of corporate governance, internal control, risk-based auditing, and organizational accountability. In this context, internal auditing is presented as a function that historically emerged from the need to prevent errors, fraud, and asset losses, but later developed into an independent and objective assurance activity concerned with governance, risk management, and control processes. This evolution has become more pronounced in the digital age, as the internal auditor's role has expanded beyond traditional control activities. The modern internal auditor is increasingly expected to analyze organizational processes, anticipate emerging risks, use digital

technologies effectively, provide reliable assurance to management, and contribute to the creation and protection of corporate value.

Digital transformation has reshaped the audit environment not only through technological change but also through methodological transformation. The digitalization of business processes, Industry 4.0 applications, cloud-based systems, remote working arrangements, ERP infrastructures, and integrated control mechanisms have changed the nature and sources of audit evidence. Physical documents, manual approval forms, and periodic reports continue to have relevance, yet they are now complemented by transaction logs, system records, electronic approval trails, automated control outputs, access reports, and database activities. This shift requires auditors to assess not only whether financial information is accurate, but also whether the systems that generate, process, store, and report that information are reliable.

Audit methodology in the digital age has increasingly moved toward a risk-oriented, data-driven, and continuous assurance structure. Traditional audit planning has often relied on annual audit programs, prior-period findings, and standard checklists. In digital audit environments, however, risk indicators, anomaly analyses, system alerts, real-time data flows, and dynamic risk dashboards play a more prominent role. As a result, the audit plan should no longer be treated as a fixed document prepared once a year. It should operate as a flexible management tool that can be updated in response to changes in the organization's risk profile. Effective internal audit functions are therefore expected to use data analytics in annual planning, allocate audit resources to high-risk areas, and adjust the audit scope in an agile manner when emerging risks require such revision.

Data analytics and artificial intelligence have become important instruments for improving the scope, timing, and depth of internal audit work. Data analytics enables auditors to move beyond narrow sample-based testing and examine full transaction populations or significantly larger datasets. This capacity supports the earlier identification of duplicate payments, unusual transaction timing, authorization breaches, split transactions below approval thresholds, abnormal inventory movements,

suspicious supplier relationships, and other potential indicators of fraud. Artificial intelligence and machine learning further contribute to risk prediction, anomaly detection, process mining, continuous transaction testing, and predictive audit applications. However, these tools should support rather than replace the auditor's professional judgment. Their outputs need to be evaluated in light of data quality, model assumptions, algorithmic bias, and explainability.

Cybersecurity and information systems auditing have also become central components of modern internal auditing. In digitalized organizations, financial reporting, payment systems, customer data, inventory management, human resources, supply chain operations, and management reporting depend heavily on information systems. Therefore, risks such as unauthorized access, data breaches, ransomware attacks, phishing, social engineering, backup failures, system interruptions, and weak incident response are no longer merely technical IT issues. They are audit-relevant risks that may directly affect financial reporting reliability, business continuity, corporate reputation, regulatory compliance, and managerial accountability. In this environment, internal audit is expected to evaluate cybersecurity control design, test incident response capabilities, analyze access management risks, review compliance with data privacy requirements, and provide independent assurance to the board of directors and senior management.

The robustness of digital internal control systems depends on the integrated consideration of technology, processes, people, and governance. ERP systems, automated controls, role-based access structures, system alerts, and digital workflows may strengthen the control environment when they are properly designed and monitored. However, these benefits can be undermined by poorly structured authorization matrices, segregation of duties conflicts, unreviewed system logs, weak data quality, ineffective automated controls, or insufficiently tested system changes. For this reason, the existence of a control in a digital system should not be confused with its actual effectiveness. A control may be formally defined in the system but still fail to operate as intended or reduce the relevant risk. The responsibility of internal

audit is therefore to evaluate control design, operating effectiveness, data reliability, and monitoring mechanisms together.

The case studies in this book offer significant insights into the practical application of theoretical discussions. Financial audit cases demonstrate how financial reporting risks can arise, particularly in areas such as revenue classification, period-end transactions, collectibility, campaign and incentive income, presentation of exchange rate gains, and verification of trade receivables. The key lesson learned from these cases is that financial manipulation often occurs not through a single transaction, but through a combination of classification preferences, period shifts, lack of documentation, failure to provide provisions, and management pressure. Therefore, the internal auditor must assess not only the technical accuracy of the accounting entry but also the economic substance of the transaction, its timing, collectibility, and its impact on reporting.

The digital procurement fraud case revealed how risks such as fraudulent suppliers, ERP manipulation, duplicate payments, lack of separation of duties, and insufficient proof of delivery for services can cause financial losses for businesses. The most important lesson learned from this case is that weaknesses in internal controls in purchasing and payment processes feed off each other. If supplier master data is opened without control, if the ERP authorization matrix is inadequate, if three-way matching controls are not functioning effectively, if there is no pre-payment duplicate invoice check, and if proof of delivery for services is weak, the risk of fraud becomes systemic. Therefore, supplier master data management, separation of duties, automated duplicate payment algorithms, approval limits, ERP log reviews, and continuous audit panels should be designed together in digital procurement processes.

The inventory management case demonstrated that using ERP systems solely as a record-keeping tool is insufficient. Discrepancies between actual inventory and ERP records, ineffective barcode verification, weak warehouse location controls, inadequate approval of manual inventory adjustments, lack of reconciliation between delivery notes, orders, and actual deliveries during the receiving process, and

the absence of separate processes for damaged/returned/waste inventory all point to weaknesses in the operational control environment. The key lesson learned from this case is that for an ERP system to be a powerful control tool, process discipline, barcode usage, job descriptions, approval mechanisms, and management reporting must all work together. Entering data into an ERP system alone is not control; control is achieved by ensuring that data is generated accurately, timely, authoritatively, and verifiably.

Human resources and ghosting employee Fraud cases highlight the importance of data integrity, employee records, access rights, and separation of duties controls in payroll processes. The risk of ghost employees is not solely a problem for the human resources department; it arises when connections are not established between payroll, accounting, bank payment files, employee onboarding and offboarding records, system user accounts, and management approvals. Such cases demonstrate the need for internal audit to compare human resources data with financial payment data. Reconciling the active employee list, payroll list, bank payment file, employee onboarding notification, employee offboarding records, and system user accounts is one of the fundamental audit procedures that reduces the risk of payroll fraud.

ERP unauthorized access and cyber audit cases demonstrate that user permissions are one of the most critical risk areas in digital systems. Excessive privileges, failure to close legacy employee accounts, neglecting to monitor privileged user accounts, shared username usage, violations of separation of duties, and lack of regular analysis of log records increase the risk of both financial errors and fraud. The common lesson from these cases is that access management cannot be narrowed down to a purely technical IT issue. User permissions must be evaluated in conjunction with business processes, approval mechanisms, control ownership, and audit evidence . Beyond knowing which user accessed which system, the internal auditor must analyze the company risks that this access poses.

Data backup and disaster recovery cases demonstrate that a business's digital resilience depends not only on systems being operational, but

also on their capacity to recover in the event of system failure or data loss. Backup alone is insufficient; regular testing of backups, establishment of recovery times, prioritization of critical systems, verification of data integrity, and testing of disaster recovery plans against realistic scenarios are necessary. The key lesson from this case is that business continuity and disaster recovery plans, when merely documented , do not provide assurance. Internal audits should evaluate the applicability and test results of these plans.

Fraud and ethics cases reveal that technological controls alone are insufficient in the digital age. Management manipulation, insider trading... Threats , confidential data leaks, employee misconduct, and misreporting under financial pressure are more likely to occur when the control environment is not supported by an ethical culture. The key lesson learned from these cases is that internal audit must consider not only control procedures but also management pressure, the ethical climate, conflicts of interest, incentive systems, and employee behavior. Ethical awareness, whistleblowing mechanisms, independent review, data access controls, and specific audit procedures to address the risk of management circumvention of controls are critical in this context.

The continuous audit, real-time assurance, future internal auditor competencies, and AI-assisted auditing discussed in the book's final chapters demonstrate the future direction of internal auditing. Continuous control monitoring, real-time audit systems, intelligent dashboards, and integrated assurance models are transforming internal auditing from a function that provides periodic reporting to an assurance system that generates continuous value. This transformation enables management to identify risks earlier, improve controls faster, and base strategic decisions on more reliable information.

Data literacy is one of the most critical competencies for the internal auditor of the future. Auditors must now be able to understand large datasets, use basic analytical techniques, identify data quality issues, and relate analytical results to business risk. In addition, technological skills have become indispensable. An internal auditor without basic knowledge of ERP systems, cybersecurity, cloud computing, artificial

intelligence, robotic process automation, blockchain, and automated control systems will struggle to evaluate digital processes with sufficient depth. However, technical knowledge alone is not enough. Analytical thinking, ethical awareness, communication skills, professional skepticism, and effective reporting capacity in digital environments are equally important.

The strategic importance of digital internal audit becomes apparent here. Digital internal audit is not simply about performing audit activities with technology. Its true strategic value lies in transforming internal audit into a function that provides assurance in the company's digital transformation process, identifies risks early, supports the embedding of controls into digital systems, and provides the board of directors with reliable information about technology-related risks. In this sense, digital internal audit is a fundamental component of corporate resilience, cybersecurity, data governance, financial transparency, and ethical management.

The strategic importance of digital internal audit lies in its capacity to transform audit activities from periodic control reviews into a more continuous, data-driven, and risk-oriented assurance function. By using data analytics and continuous monitoring mechanisms, internal audit improves the visibility of risks across business processes and enables management to identify control weaknesses before they escalate. The evaluation of automated controls, ERP workflows, authorization matrices, and system alerts further contributes to the reliability of the control environment. Digital audit techniques also expand fraud detection capacity by revealing anomalies, unusual transaction patterns, and behavioral indicators that are difficult to detect through conventional audit procedures. Beyond these areas, internal audit plays an important role in strengthening cyber resilience by assessing cybersecurity governance, access controls, backup arrangements, incident response processes, and data protection practices. As audit findings become more timely, visual, and evidence-based, they provide management with clearer insights and support more effective strategic and operational decision-making.

However, the digital internal audit transformation also carries some risks. Over-reliance on technology can lead to the creation of false assurances. Just because a system operates automatically doesn't mean it operates flawlessly. An AI model generating a risk score doesn't mean that score is correctly interpreted. The existence of defined controls in an ERP system doesn't mean those controls are effective. Therefore, the fundamental principle of digital internal audit should not be to replace the auditor with technology, but to strengthen the auditor's professional judgment. The auditor should question the data provided by the technology, evaluate the system's output within the company context, and independently form the final assurance judgment.

In conclusion, the overall assessment reached in this book is this: In the digital age, internal audit is not only a control function for businesses but also a fundamental element of their strategic governance capacity. Internal audit should be positioned as a function that strengthens corporate governance, evaluates internal control systems, anticipates risks, secures technological transformation, makes fraud and ethical risks visible, supports cyber resilience, and adds value to management. This positioning makes the independence, objectivity, and adherence to professional standards of internal audit even more important.

Digitalization is not eliminating internal audit; on the contrary, it is increasing its importance. Because as technology use increases, businesses generate more data, processes become more complex, controls are embedded in systems, and risks spread more rapidly. In this environment, managers, audit committees, and stakeholders have an even greater need for a reliable, independent, and technologically competent internal audit function. The successful organizations of the future will be those that view internal audit not merely as a formality for regulatory compliance, but as a strategic partner ensuring that digital transformation is carried out in a secure, ethical, controlled, and sustainable manner.

Therefore, the future of internal audit will be shaped by a combination of risk-focused thinking, data-driven analysis, continuous

assurance, ethical sensitivity, technological literacy, and independent professional judgment. In the digital age, strong internal audit is not merely a function that shows what went wrong; it is a strategic assurance mechanism that anticipates what could go wrong, strengthens control systems, alerts management in a timely manner, and contributes to the creation of corporate value.

References

Adeboye, E. O., Ifeanyi, E. V., & Labisi, G. (2021). Redesigning internal controls for small enterprises: A COSO-based framework for fraud prevention and regulatory compliance. Iconic Research and Engineering Journals, 4(9), 334–344.

Adesokan-Imran, T. O. (2025). The impact of cybersecurity governance on national security by strengthening critical infrastructure through IT auditing and risk management. Asian Journal of Research in Computer Science, 18(4), 301–322. https://doi.org/10.9734/ajrcos/2025/v18i4621

Aditya, B. R., Hartanto, R., & Nugroho, L. E. (2018, August). The role of IT audit in the era of digital transformation. In IOP Conference Series: Materials Science and Engineering (Vol. 407, No. 1, p. 012164). IOP Publishing.

Adriansyah, Rais, A. H., & Windarsari, W. R. (2025). Professionalism of accountants in the digital era: Ethics, competence, and public trust. Review of Accounting and Business, 5(1), 45–58.

Aeni, N., & Mais, R. G. M. R. G. (2026). The role of information technology in enhancing cybersecurity and audit quality for external auditors in public accounting firms. Jurnal Akuntansi STEI, 12(1), 17-32.

Ahmed, E. M., & Japee, G. P. (2025). The evolving role of internal audit in the digital era (2019 to 2025): A systematic review of artificial intelligence (AI), data analytics, and cybersecurity practices. Inspira-Journal of Commerce, Economics & Computer Science, 11(3), 213–227. https://doi.org/10.62823/jcecs/11.03.8040

Akatak, A. (2025). The future of internal auditing with AI capabilities. In AI-driven accounting transformation: A new era for management and auditing (pp. 29–42). Nobel Akademik Yayıncılık.

Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S. (2021). Integrated framework for cybersecurity auditing. Information Security Journal: A Global Perspective, 30(4), 189-204.

Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S. (2018, October). Cybersecurity tools for IS auditing. In 2018 Sixth international conference on enterprise systems (ES) (pp. 217-223). IEEE.

Al-Omush, A., Almasarwah, A., & Al-Wreikat, A. (2025). Artificial intelligence in financial auditing: redefining accuracy and transparency in assurance services. EDPACS, 70(6), 1-20.

Ali, M. M., Abdullah, A. S., & Khattab, G. S. (2022). The effect of activating artificial intelligence techniques on enhancing internal auditing activities: Field study. Alexandria Journal of Accounting Research, 6(3), 1–40.

Alsagoor, M. H., Daud, Z. B. M., & Osman, M. N. H. B. (2024). Digital transformation, emotional intelligence, and organizational culture toward internal audit quality: Conceptual framework. Advances in Social Sciences Research Journal, 11(7), 92–108. https://doi.org/10.14738/assrj.117.17271

Alwyah, L. (2025). The role of internal audit in enhancing good corporate governance. INPAC: Journal of Innovative Public Accounting and Complience, 1(1), 17–26.

Alzeban, A., Al-Hajaya, K., Sawan, N., Chammaa, H., & Foster, S. (2026). The quality of cybersecurity audits: Do synergies among the chief audit executive, IT governance and internal audit functions matter? *Managerial Auditing Journal, 41*(2), 322–349. https://doi.org/10.1108/MAJ-05-2025-4825

Amo, H. F., Tetteh, L. A., Owusu, G. M. Y., Agyenim-Boateng, C., & Amankwa, R. F. (2026). Drivers of value of internal audit function: The perception of internal auditors and other primary stakeholders. Journal of Economic and Administrative Sciences. https://doi.org/10.1108/JEAS-05-2025-0246

Andreanov, & Maisyarah, R. (2025). Cybersecurity audit and IT risk management. 2nd International Conference on Islamic Community Studies (ICICS), 64–76.

Ansari, A., Valipour, H., & Salehi, H. (2025). The Impact of Artificial Intelligence Algorithms on Financial Fraud Detection and Prevention: The Moderating Role of Internal Control Systems. International Journal of Finance & Managerial Accounting, 12(47), 93-110.

Antunes, M., Maximiano, M., & Gomes, R. (2022). A client-centered information security and cybersecurity auditing framework. Applied Sciences, 12(9), 4102. https://doi.org/10.3390/app12094102

Antunes, M., Maximiano, M., & Gomes, R. (2022). A customizable web platform to manage standards compliance of information security and cybersecurity auditing. Procedia Computer Science, 196, 36–43. https://doi.org/10.1016/j.procs.2021.11.070

Ayoub, E. L., Charef, F., & Bourjila, M. (2025). The impact of digital transformation on the internal audit function: A literature review. International Journal of Accounting Finance Auditing Management and Economics, 6(7), 354–366.

Baharom, Z. (2025). The transformative role of artificial intelligence in internal auditing: A critical review. International Journal of Research and Innovation in Social Science, IX(VI), 2953–2966. https://doi.org/10.47772/IJRISS.2025.906000217

Bani, P., Siregar, N., Subiyanto, B., & Awaludin, D. T. (2025). Digital transformation in the audit process: A systematic review of innovation, challenges, and its impact on audit quality. JRSSEM, 5(3), 3454–3471.

Batte, B. (2025). COSO framework in the digital age: Strengthening internal controls and IT audits. SSRN. https://ssrn.com/abstract=5320726

Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. Computer Science & IT Research Journal, 5(6), 1505–1520.

Betti, N., & Sarens, G. (2021). Understanding the internal audit function in a digitalised business environment. Journal of Accounting & Organizational Change, 17(2), 197–216.

Boubouh, I., & Ghanim, M. (2025). Internal controls in the digital age: Simplification or complication? International Journal of Research in Economics and Finance, 2(2), 149–163. https://doi.org/10.71420/ijref.v2i2.63

Calvin, C., Eulerich, M., & Holt, M. (2025). Characteristics of cybersecurity and IT involvement by the IA activity. International Journal of Accounting Information Systems, 56, 100726. https://doi.org/10.1016/j.accinf.2025.100726

Daidj, N. (2022). The digital transformation of auditing and the evolution of the internal audit. Routledge.

Dhahir, D. A. B., Qassim, O. A., & Abbas, S. R. (2025). The role of the internal control system in light of the electronic operation of accounting

data. American Journal of Economics and Business Management, 8(3), 1257–1268.

Djogo, Y. O. (2023). Internal auditor human resources development strategy in the era of disruption. ATESTASI: Jurnal Ilmiah Akuntansi, 6(2), 627–639. https://doi.org/10.57178/atestasi.v6i2.723

Eklöv Alander, G., & Holmgren Caicedo, M. (2026). Internal auditors' independence tactics: Defending the third line in Swedish public sector agencies. Accounting, Auditing & Accountability Journal, 39(9), 215–240. https://doi.org/10.1108/AAAJ-01-2024-6866

Emran, A. K. M., & Rubel, M. T. H. (2024). Big data analytics and AI-driven solutions for financial fraud detection: Techniques, applications, and challenges. Frontiers in Applied Engineering and Technology, 1(01), 269–285.

Espinosa-Jaramillo, M. T. (2024). Internal control in companies from the perspective of the COSO. Management (Montevideo) = AG Management, 2, Article 28. https://doi.org/10.62486/agma202428

Ez-Zaidi, A., & Ghandari, Y. (2023). Audit profession and innovation: Emerging practices in the era of digital transformation and their relationship to the environment. In E3S Web of Conferences (Vol. 412, p. 01010). EDP Sciences.

Fang, Q., Wang, Z., & Dang, L. (2025). Audit effort in the digital era: Uncovering the dynamic interplay of business strategy and digital transformation. International Journal of Accounting Information Systems, 56, 100747.

Farhan, K. A., & Kawther, B. I. (2023). Accounting audit profession in digital transformation environment between theoretical framework and practical reality. World Economics & Finance Bulletin, 22, 120–133.

Farras, A., Ali, A., & Audi, M. (2025). Advancing audit practices through technology: A comprehensive review of continuous auditing. Journal of Social Signs Review, 3(2), 506–539.

Ferdia, M. S., & Kammoun, A. (2024). Conceptual framework of internal control. Psychology and Education, 61(8), 1459–1471.

Fırat, Z. (2025). Artificial intelligence in auditing: Opportunities, challenges, and future directions. Muhasebe Bilim Dünyası Dergisi, 27(2), 77–95. https://doi.org/10.31460/mbdd.1577715

Ghafar, I., Perwitasari, W., & Kurnia, R. (2024). The role of artificial intelligence in enhancing global internal audit efficiency: An analysis. Asian Journal of Logistics Management, 3(2), 64–89.

Gökoğlan, K., Sevim, H., & Kılıç, S. (2025). Digital transformation and artificial intelligence-assisted auditing: The role of technology in internal audit processes in 2025. Dynamics in Social Sciences and Humanities, 6(1), 25–33. https://doi.org/10.62425/dssh.1647929

Green, I. (2023). The Impact of Digital Transformation on Accounting and Auditing Functions. gjstudies, 1(1), 7-7.

Guliyeva, A., & Gaziyeva, G. (2025). Audit planning in the context of digital transformation. Scientific Collection «InterConf», (250), 53–59. Retrieved from https://archive.interconf.center/index.php/conference-proceeding/article/view/7160

Hallak, J., & Feghali, K. (2026). The impact of chaos and cultural theories on the internal audit environment in a context of cultural change: An international study. Journal of Accounting & Organizational Change. https://doi.org/10.1108/JAOC-11-2024-0384

Hassan, M. O. M. (2025). The use of artificial intelligence techniques and their impact on the independence of the internal auditor and the quality of electronic financial reports. Available at SSRN 5403606.

Huang, L.-H. (2026). Evaluating the internal control strategy in the AI industry: Using the COSO framework. Applied Economics, 58(1), 172–185. https://doi.org/10.1080/00036846.2025.2451255

Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Advanced data analytics in internal audits: A conceptual framework for comprehensive risk assessment and fraud detection. Finance & Accounting Research Journal, 6(6), 931–952.

Iseal, S., Joseph, O., & Joseph, S. (2025). AI in financial services: Using big data for risk assessment and fraud detection. vol, 2, 1-21.

Ishaku, A., Shuaibu, K., Yusuf, A., & Lawal, S. (2023). Disruptive technologies and internal audit: A conceptual review. In Sustainable Transformation of Public and Corporate Management in Digital Age: Perspectives, Challenges & Prospects (p. 107). Bayero University Kano.

Kabuye, F., Nkundabanyanga, S. K., Kaawaase, T. K., Nalukenge, I., Nakyeyune, G. K., & Ngoboka, P. (2026). Exploring the effect of internal audit quality on fraud management: The mediating role of ethical

behaviour in public sector institutions. IIM Ranchi Journal of Management Studies, 1-23. https://doi.org/10.1108/IRJMS-08-2025-0105

Kabuye, F., Nkundabanyanga, S. K., Opiso, J., & Nakabuye, Z. (2017). Internal audit organisational status, competencies, activities and fraud management in the financial services sector. Managerial Auditing Journal, 32(9), 924–944.

Kagermann, H., Kinney, W., Küting, K., & Weber, C.-P. (Eds.). (2008). Internal audit handbook: Management with the SAP audit roadmap. Springer.

Laflafli, S., & Saidi, C. (2025). The contribution of internal audit to the enhancement of corporate governance. Revue Internationale des Sciences de Gestion, 8(3), 1087–1109.

Leng, A., & Zhang, Y. (2024). The effect of enterprise digital transformation on audit efficiency—Evidence from China. Technological Forecasting and Social Change, 201, 123215.

Li, H., Freitas, M. M. D., Lee, H., & Vasarhelyi, M. (2024). Enhancing continuous auditing with large language models: AI-assisted real-time accounting information cross-verification. Available at SSRN 4692960.

Lotfy, A. E. A. (2026). An XAI-driven digital twin audit framework for cybersecurity risk assurance: Empirical evidence from the Egyptian Exchange. Journal of Economics, Finance and Management Studies, 9(4), 1888–1921. https://doi.org/10.47191/jefms/v9-i4-21

Loumachi, F. Y., Lacerda, M. J., Ouazzane, K., Adnane, A., & Adamyk, O. (2026). AI in control: Rethinking cybersecurity compliance and auditing. Information and Software Technology, 195, 108132. https://doi.org/10.1016/j.infsof.2026.108132

Luckyanayu, I. H., Huda, A. N., & Mappadang, A. (2025). Strengthening corporate governance through the strategic role of internal audit: A systematic literature review. Journal of Principles Management and Business, 4(2), 304–317.

Ma, Y., & Zhang, H. (2026). Digital transformation and internal audit quality and efficiency: Dual pathways through human capital and financial channels. Asian Review of Accounting. https://doi.org/10.1108/ARA-07-2025-0252

Manita, R., Elommal, N., Baudier, P., & Hikkerova, L. (2020). The digital transformation of external audit and its impact on corporate governance. Technological Forecasting and Social Change, 150, 119751.

Mat Ridzuan, N. I., Said, J., Mohd Razali, F., Abdul Manan, D. I., & Sulaiman, N. (2022). Examining the role of personality traits, digital technology skills and competency on the effectiveness of fraud risk assessment among external auditors. Journal of Risk and Financial Management, 15(11), Article 536. https://doi.org/10.3390/jrfm15110536

Mintah, R., Bekoe, R. A., & Owusu, G. M. Y. (2025). The interplay of sociocultural determinants and internal audit activities in mitigating public sector fraud. Journal of Accounting in Emerging Economies, 15(5), 1110–1131. https://doi.org/10.1108/JAEE-04-2024-0162

Mo, H. (2023). The impact of digital transformation on internal control quality: A study based on five components of internal control. Accounting and Corporate Management, 5(4), 28–34. https://doi.org/10.23977/acccm.2023.050405

Muhammad, A. E., Yow, K.-C., & Alsenan, S. (2026). Audit-as-code: A policy-as-code framework for continuous AI assurance. Frontiers in Artificial Intelligence, 9, Article 1759211. https://doi.org/10.3389/frai.2026.1759211

Muthusamy, M. (2024). Cloud-native AI metrics model for real-time banking project monitoring with integrated safety and SAP quality assurance. International Journal of Research and Applied Innovations, 7(1), 10135-10144.

Nandal, N. (2026). AI-governed audit assurance: A conceptual framework integrating predictive intelligence, governance controls, and continuous assurance. EDPACS, 1–21. https://doi.org/10.1080/07366981.2026.2667950

Omolere, O. (2025). The role of continuous auditing in managing cyber threats: Analyzing how real-time monitoring and continuous audit models improve detection of cyber incidents. SSRN. https://ssrn.com/abstract=5999855.

Putra, I., Sulistiyo, U., Diah, E., Rahayu, S., & Hidayat, S. (2022). The influence of internal audit, risk management, whistleblowing system and big data analytics on the financial crime behavior prevention. Cogent Economics & Finance, 10(1), 2148363.

Qatawneh, A. M. (2024). The role of artificial intelligence in auditing and fraud detection in accounting information systems: Moderating role of natural language processing. International Journal of Organizational Analysis, 33(6), 1391-1409.

Ramamoorti, S. (2003). Internal auditing: History, evolution, and prospects. In A. D. Bailey, A. A. Gramling, & S. Ramamoorti (Eds.), Research opportunities in internal auditing (pp. 1–23). The Institute of Internal Auditors Research Foundation.

Raza, M., Qurashi, H., Haidar, A., & Raza, M. S. (2025). Artificial intelligence in auditing: Transforming fraud detection, risk assessment and assurance quality in financial reporting. Journal of Asian Development Studies, 14(3), 453–466. https://doi.org/10.62345/jads.2025.14.3.38

Roussy, M., & Perron, A. (2018). New perspectives in internal audit research: A structured literature review. Accounting Perspectives, 17(3), 345–385. https://doi.org/10.1111/1911-3838.12180

Rumasukun, M. R. (2024). Developing auditor competencies through continuous training and education. Golden Ratio of Auditing Research, 4(1), 14–23. https://doi.org/10.52970/grar.v4i1.384

Saat, M. M., Zulkarnaini, N. A. S. B., & Lie, T. L. (2025). The effects of cloud computing and cybersecurity skills on accountants' employability in the digital era: Towards research agenda. International Journal of Research and Innovation in Social Science, 9(14).

Sadek, A. A., Farag, O. M. Y., & Mahmoud, A. A. (2024). The effect of the continuous audit on the quality of external audit in the digital transformation environment. Journal of Contemporary Business Research, 1(1), 75–100.

Samuel, A. J. (2023). Enhancing financial fraud detection with AI and cloud-based big data analytics: Security implications. World Journal of Advanced Engineering Technology and Sciences, 9(2), 417–434. https://doi.org/10.30574/wjaets.2023.9.2.0208

Shafa, H., & Islam, A. (2025). Impact of data privacy and cybersecurity in accounting information systems on financial transparency. International Journal of Scientific Interdisciplinary Research, 6(1), 254–292. https://doi.org/10.63125/xs0xt970

Shah, A. A., Azmat, M., Rasheed, Q.-U.-A., & Arshad, A. (2023). Impact evaluation of factors of internal audit on internal audit effectiveness:

The moderating and mediating effect of ethical culture and internal controls. Pakistan Journal of Humanities and Social Sciences, 11(1), 490–506. https://doi.org/10.52131/pjhss.2023.1101.0367

Shakkur, M. R. (2023). The impact of enterprise resource planning (ERP) systems on achieving the effectiveness of internal control for companies: Case study General Motors. *World Economics & Finance Bulletin, 25*, 37–46.

Shivram, V. (2024). Auditing with AI: A theoretical framework for applying machine learning across the internal audit lifecycle. EDPACS, 69(1), 22–40. https://doi.org/10.1080/07366981.2024.2312025

Siyaya, M. C., Dubihlela, J., & Sibanda, M. (2025). A literature review of internal auditing involvement in cybersecurity risk management of the organisation. Journal of Contemporary Management, 22(Special Issue 1), 89–115. https://doi.org/10.35683/jcm24.030.293

Stepanyan, S. (2023). The evolution of internal audit in a digital environment. Alternative Quarterly Academic Journal, 151–156.

Syahputra, R. M. (2022). Analysis of the role of internal audit in enhancing company's internal control. Golden Ratio of Auditing Research, 2(1), 42–52. https://doi.org/10.52970/grar.v2i1.371

Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The role of big data in detecting and preventing financial fraud in digital transactions. World Journal of Advanced Research and Reviews, 22(02), 1746–1760.

Usul, H., & Alpay, B. Y. (2025). Digital transformation in internal audit: Paradigm shifts, emerging risks, and strategic resilience. European Journal of Digital Economy Research, 6(1), 23–36. https://doi.org/10.5281/zenodo.15660150

Vuko, T., Slapničar, S., Čular, M., & Drašček, M. (2025). Key drivers of cybersecurity audit effectiveness: A neo-institutional perspective. International Journal of Auditing, 29(1), 188–206. https://doi.org/10.1111/ijau.12365

Wassie, F.A., Lakatos, L.P. Artificial intelligence and the future of the internal audit function. Humanit Soc Sci Commun 11, 386 (2024). https://doi.org/10.1057/s41599-024-02905-w

Wronka, A. (2019). The emotional aspect of an internal audit. Journal of Positive Management, 10(3), 20–30. https://doi.org/10.12775/JPM.2019.015

Zhao, C., & Xu, J. (2025). Corporate governance, internal audit quality and corporate value. In W. Zang & C. Xia (Eds.), Proceedings of the 2025 3rd International Conference on Digital Economy and Management Science (pp. 288–293). Atlantis Press. https://doi.org/10.2991/978-94-6463-770-0_34

Acknowledgements

This book was originally prepared in Turkish. Generative AI tools were used to support the translation and language editing of the English version. The final text was reviewed and approved by the author, who assumes full responsibility for its content.

About the Book Series

Contemporary Studies in Business and Management is a double-blind peer-reviewed academic book series dedicated to interdisciplinary research in business, management, accounting, finance, marketing, entrepreneurship, human resource management, organizational behavior, strategic management, sustainability, digital transformation, and related fields. The series welcomes theoretical, empirical, and applied studies across diverse sectors, including tourism, healthcare, finance, education, manufacturing, retail, technology, and public administration. It provides a platform for innovative research on contemporary challenges and emerging trends, such as artificial intelligence, corporate sustainability, ethical leadership, international business, consumer behavior, and strategic decision-making, fostering scholarly dialogue and contributing to global academic knowledge.

About the Editors

Tuğçe Uzun Kocamış is an Associate Professor at Istanbul University-Cerrahpaşa. She holds a Ph.D. in Business Administration and has professional experience in internal auditing and senior management. Her research focuses on accounting, auditing, taxation, international accounting, and sustainability.
Ali Kuzu is an Associate Professor at Istanbul University-Cerrahpaşa. He holds a Ph.D. in Production Management and Marketing and has extensive private-sector experience. His research interests include management and organization, organizational behavior, and service quality management.
Serap Özdemir Güzel is an Associate Professor at Istanbul University-Cerrahpaşa specializing in tourism management, marketing, and sustainable tourism. She has participated in numerous TÜBİTAK and Erasmus+ research projects as a researcher and expert.

About the author of this volume

Tuğçe Uzun Kocamış graduated from Istanbul University, Faculty of Business Administration, Department of Business Administration (1996). She received her master's degree (2001) from Istanbul University, Institute of Social Sciences, Department of Business Administration, and her Ph.D. (2015) from Marmara University, Institute of Social Sciences, Department of Business Administration. She is currently working as an Associate Professor at the Accounting and Tax Applications Program of Istanbul University-Cerrahpaşa. She started her professional career as an internal auditor and held senior management positions in the private sector for many years. She has participated in several national projects and has served as a researcher and expert in Erasmus+ KA227 and two KA220 projects. Her research focuses on accounting, international accounting, auditing, taxation, and sustainability.