



This is a peer-reviewed, final published version of the following document, Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>). and is licensed under Creative Commons: Attribution 4.0 license:

Metin, Bilgin, Berfun Sevim, Sibel and Wynn, Martin G ORCID logoORCID: <https://orcid.org/0000-0001-7619-6079> (2025) Cybersecurity Strategy Development: Towards an Integrated Approach Based on COBIT and ISO 27000 Series Standards. Standards, 5 (4). art 033. doi:doi.org/10.3390/standards5040033

Official URL: <https://doi.org/10.3390/standards5040033>

DOI: doi.org/10.3390/standards5040033

EPrint URI: <https://eprints.glos.ac.uk/id/eprint/15650>

Disclaimer

The University of Gloucestershire has obtained warranties from all depositors as to their title in the material deposited and as to their right to deposit such material.

The University of Gloucestershire makes no representation or warranties of commercial utility, title, or fitness for a particular purpose or any other warranty, express or implied in respect of any material deposited.

The University of Gloucestershire makes no representation that the use of the materials will not infringe any patent, copyright, trademark or other property or proprietary rights.

The University of Gloucestershire accepts no liability for any infringement of intellectual property rights in any material deposited but will remove such material from public view pending investigation in the event of an allegation of any such infringement.

PLEASE SCROLL DOWN FOR TEXT.

Article

Cybersecurity Strategy Development: Towards an Integrated Approach Based on COBIT and ISO 27000 Series Standards

Bilgin Metin ¹, Sibel Berfun Sevim ¹ and Martin Wynn ^{2,*}

¹ Management Information Systems Department, Bogazici University, Istanbul 34342, Turkey; bilgin.metin@bogazici.edu.tr (B.M.); berfun.aslan.2021@alumni.bogazici.edu.tr (S.B.S.)

² School of Business, Computing and Social Sciences, University of Gloucestershire, Cheltenham GL502RH, UK

* Correspondence: mwynn@glos.ac.uk

Abstract

This article presents a practical guide for developing a cybersecurity strategy that integrates COBIT 2019 with the ISO/IEC 27000 series of standards. Although COBIT 2019 provides strong frameworks for IT strategy and governance, it does not specifically prescribe a cybersecurity strategy. This article addresses this gap in the strategy literature by building upon the ISO/IEC 27000 series, which is designed to be adaptable for organizations of all types and sizes, as well as being suitable for various regulatory and technological environments. First, a synthesis of COBIT 2019 and the ISO/IEC standards (particularly 27014, 27001, 27036, and 27701) identifies six key themes for a cybersecurity strategy. A more specific qualitative content analysis of ISO/IEC 27014 (which focuses on board-level information security governance) and COBIT 2019 (which outlines execution mechanics) confirms the validity of these themes with traceability at the clause and objective levels. To operationalize these themes, a three-step method is put forward: setting alignment objectives and scope; translating these into IT strategy decisions using COBIT governance and management objectives and practices; and establishing a cybersecurity strategy through ISO/IEC 27001. Additionally, ISO/IEC 27701 for privacy and ISO/IEC 27036 for supplier governance are incorporated where relevant. An illustrative example is provided using anonymized data from public sources, and the applicability and limitations of the research findings are discussed.



Academic Editor: Gilberto Santos

Received: 3 October 2025

Revised: 21 November 2025

Accepted: 27 November 2025

Published: 5 December 2025

Citation: Metin, B.; Sevim, S.B.; Wynn, M. Cybersecurity Strategy Development: Towards an Integrated Approach Based on COBIT and ISO 27000 Series Standards. *Standards* **2025**, *5*, 33. <https://doi.org/10.3390/standards5040033>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: IT strategy; cybersecurity strategy; digitalization; business objectives; IT governance; COBIT; strategy alignment; ISO 27001; ISO 27014; ISO 27036; ISO 27701

1. Introduction

The development and deployment of digital technologies continue to expand in business, as well as in wider society. These advancements offer significant benefits but also introduce new vulnerabilities that should be proactively addressed. The potential impact of such threats was illustrated in September 2025, when Jaguar Land Rover (JLR), Britain's biggest car maker, suffered a cyberattack that halted production at three UK factories. The UK government has made a £ 1.5 billion rescue fund available to the company "after hackers breached the company's IT systems" [1] (p. 2). Developing a robust cybersecurity strategy has now become a strategic necessity to safeguard against such potential threats, which can severely threaten an organization's business continuity. Data breaches damage a company's reputation, and considerable costs can be incurred by the infrastructure works carried out to recover from such events and then prevent them from happening

again. Cybersecurity is now not only an IT issue but is increasingly accepted as a broader business concern, prompting organizations to develop and implement a cybersecurity strategy. As the pace and impact of digitalization accelerate, almost all organizations will face cyberattacks and need to protect their critical data, supply chain operations, and IT infrastructures. This requires the alignment of a cybersecurity strategy with business and IT objectives to optimize the use of IT resources and comply with internal and external business regulations. This article focuses on one possible approach to meeting this challenge, which is the application of the Control Objectives for Information and Related Technology (COBIT) [2] framework in conjunction with the adoption of specific ISO standards.

The need for an alignment of business objectives with IT strategy is well documented [3–5] and can be traced back to Earl's [6] classic model of IT and IS strategy development, and more recent studies have highlighted the requirement for an aligned cybersecurity strategy [7]. However, there are few sources that directly set out a comprehensive approach to cybersecurity strategy development, and it is this gap that this article addresses. More specifically, the article answers the following research questions (RQs):

RQ1. How do COBIT and the ISO 27000 [8] series of standards relate to cybersecurity issues?

RQ2. How can these standards be combined and utilized in the strategy development process?

While COBIT 2019 excels at IT strategy and governance, it does not prescribe a cybersecurity strategy. This is addressed by integrating ISO/IEC 27014 [9] with COBIT's governance/management objectives and operationalizing the result—together with ISO/IEC 27001/27036/27701 [10–15]—into a three-step, evidence-based method that is applied using an illustrative company IT strategy (Appendix A: Table A1).

The article comprises six sections. Following this brief introduction, the research methodology is set out in Section 2. Section 3 then reports on relevant literature sources, examines the COBIT and ISO 27000 texts, and identifies the key concepts for subsequent analysis. In Section 4, the two RQs are addressed, and some emergent issues are briefly discussed in Section 5. Section 6 provides a conclusion to the study, summarizes the key issues raised in the article, and points out future areas for related investigation and analysis.

2. Research Method

This study utilizes a qualitative, inductive research design to ensure both academic rigor and practical applicability in developing a cybersecurity strategy approach that integrates COBIT and ISO standards. There were two phases in the research process (Figure 1). In Phase 1, a narrative literature synthesis was conducted to set the organizational and governance context [16,17], and a directed qualitative content analysis (QCA) was applied to a coded corpus comprising COBIT 2019 (Governance & Management Objectives) and ISO/IEC 27014:2020. In addition, ISO/IEC 27001:2022, ISO/IEC 27036 (supplier relationships), and ISO/IEC 27701:2025 (PIMS) were used contextually to inform interpretation but were not part of the coded corpus unless explicitly noted. This Phase 1 work resulted in a provisional conceptual framework for a more detailed assessment and integration of existing standards. In Phase 2, this outline framework was applied in an illustrative example, where a three-step process was set out to assess usability and coherence in practice. These two phases are discussed in more detail below.

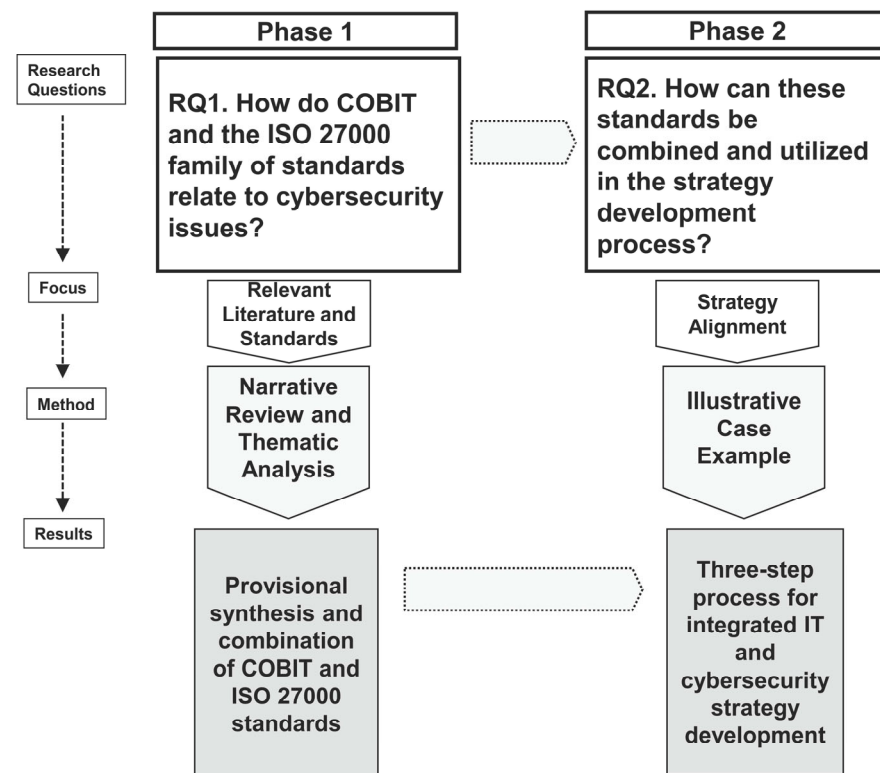


Figure 1. The two-phase research process.

2.1. Phase 1: Narrative Synthesis and Qualitative Content Analysis

Narrative synthesis is a qualitative approach that involves carefully examining and integrating findings from multiple studies. This methodology places an emphasis on the interpretative aspects of research, typically involving case studies, documented standards and regulations, and firsthand data as well as the recent literature of relevance. According to Popay et al. [18], “narrative synthesis relies on the use of words and text to summarise and explain the findings of multiple studies, rather than relying solely on numerical data”. It allows researchers to investigate patterns, relationships, and themes that are present across a variety of sources, engendering a thorough understanding of the research challenge. Here, the narrative synthesis facilitated the interpretation of complex findings from the extant literature, regulations and standards. This is accomplished by structuring the synthesis through the use of concept mapping and textual descriptions. Petticrew and Roberts [19] point out that “narrative synthesis is particularly valuable when studies vary in design, population, or intervention, as it enables researchers to construct a coherent story from fragmented evidence”.

Narrative literature synthesis focuses on the integration and interpretation of findings rather than on reporting database search strings; accordingly, the scope and selection logic (inclusion/exclusion criteria; purposive/theoretical sampling with snowballing) are set out here rather than search strings. Inclusion criteria were: enterprise-level governance/strategy relevance; explicit links to performance, risk/compliance, or stakeholder accountability; and standards with organization-wide scope. Exclusion criteria were: academic studies other than widely adopted standards and authoritative best-practice documents (e.g., ISO/IEC, ISACA) (such materials were used only contextually where needed). The selection approach was purposive/theoretical sampling informed by the authors’ practitioner experience, complemented by backward/forward snowballing.

Building on this synthesis, directed qualitative content analysis (QCA) was applied to a coded corpus comprising COBIT 2019 (Governance & Management Objectives) and

ISO/IEC 27014:2020 (Governance of Information Security) to derive and stabilise the categories used. COBIT 2019 and ISO/IEC 27014:2020 were selected for the QCA specifically because both are governance-centric; furthermore, ISO/IEC 27014:2020 provides a principled bridge to relate the strategy and governance concepts to other standards in the ISO/IEC 27000 series. ISO/IEC 27001:2022, ISO/IEC 27036 (supplier relationships), and ISO/IEC 27701:2025 (PIMS) were used contextually to inform interpretation and the case study and were not part of the coded set unless explicitly noted.

The coded corpus comprises COBIT 2019 (Governance & Management Objectives) and ISO/IEC 27014:2020. ISO/IEC 27001/27036/27701 are used contextually but are not coded. The codebook, rules, and example excerpts are provided in Appendix B (Tables A2–A4), with per-category coding counts in Table A5. The QCA findings are reported in Section 4.1.

The literature review focused on key themes such as IT strategy alignment, cybersecurity, and the security vulnerabilities introduced by digitalization, as well as an analysis of the complementarities and differences between the COBIT 2019 framework [2] and a number of ISO standards, but notably the ISO/IEC 27014 standard. This provided the basis for the development of a provisional conceptual framework, outlined below in Section 3.4.

To systematically explore the complementarities and gaps between the COBIT framework and the ISO 27000 series standards, a qualitative content analysis was conducted. Utilizing Mayring’s structured approach [20] and Schreier’s practical guidelines [21], this analysis was applied to a carefully defined set of governance documents. The selection of these documents was based on their direct relevance to governance. More specifically, the integration of COBIT 2019 (focusing on IT governance) with ISO/IEC 27014 (centered on information security governance) was to facilitate a comprehensive and practical approach to cybersecurity strategy development.

For COBIT 2019, the Governance and Management Objectives document formed the primary corpus, as it comprehensively outlines 40 governance and management objectives structured across five areas of activity (called “domains”). These domains provide detailed guidance on how IT governance supports business objectives and are directly relevant to the development of a cybersecurity strategy. Supporting COBIT documents, such as the Design Guide and Implementation Guide, were used as contextual references but were not subjected to systematic coding to maintain analytical focus.

For ISO/IEC 27014, the entire document was included in the analysis, since its scope is focused exclusively on governance of information security and it is relatively concise, with well-defined objectives (e.g., entity-wide information security, risk-based decision making, conformance, fostering a security culture, and performance monitoring) and processes (evaluate, direct, monitor, communicate). Its principles, processes, and role definitions provide a normative foundation for information security governance, making a comprehensive analysis both necessary and feasible.

Key concepts were identified in the PCF derived from the COBIT framework and the ISO/IEC 27000 series standards noted above. Segments from COBIT and ISO/IEC 27014 were coded against these categories, enabling systematic comparison and synthesis.

2.2. Phase 2: Illustrative Case Example

A documented and anonymized case example was used to illustrate the integrated cybersecurity strategy governance model developed in phase 1. The example is derived from public sources, including investor reports and press releases from a publicly listed quick service restaurant (QSR) group, as well as a published success story on cloud modernization. These sources were cross-referenced for consistency. The artifacts noted in Appendices A and B were constructed by the authors to demonstrate how the framework can be operationalized. They are not internal company documents, and no claims are

made regarding the company's implementation of the framework during the observed period. This is in line with the similar use of case examples used for both teaching and research [22,23].

The case study company is an international business operating on a global scale in the fast-food sector. It provides employment for approximately 7500 people at its headquarters and restaurants in Turkey. In addition, the company operates with more than 700 restaurants in the Turkish market, generating estimated annual sales of approximately USD 240 million. Digital channels account for 70% of all orders, with online delivery representing 85% of delivery sales, reflecting a technology-driven and customer-centric operational model.

The company maintains a streamlined yet strategically focused IT function of approximately 30–35 full-time professionals. The Head of Technology reports directly to the CEO and works in close alignment with the Chief Marketing & Digital Officer to drive a customer-centric digital agenda. The IT organization is structured around core capabilities: application development (including mobile, web, and CRM systems), cloud infrastructure on Azure Kubernetes Service (AKS), data analytics, and cybersecurity. While strategic architecture and product innovation are managed internally, infrastructure operations, DevOps pipelines, and real-time monitoring (via Prometheus, Grafana, Alertmanager, and New Relic) are supported through a partnership with a national managed services provider.

Cybersecurity responsibilities are embedded within the IT team, with an internal security lead handling day-to-day operations and compliance for privacy, while strategic oversight and risk governance rest with the technology executive and are reviewed at the executive committee level, consistent with the company's obligations as a publicly listed entity.

3. Relevant Literature and Standards

This section reports on an analysis of the literature and relevant standards based on the inclusion and exclusion criteria noted above, complemented by backward/forward snowballing. The reported literature is covered in three main sections: Section 3.1 discusses issues of relevance regarding digitalization and cybersecurity. Then, in Section 3.2, strategy alignment and integration are examined. This is followed in Section 3.3 by a review of the relevant IT governance frameworks and standards. Finally, the emergent themes from the assessment of relevant standards and frameworks are brought together in Section 3.4 in a provisional conceptual framework for the subsequent research phase.

3.1. Digital Technologies and Cybersecurity (Contextual Background)

The benefits and threats associated with different digital technologies (Figure 2) vary. For example, Internet of Things (IoT) devices, especially those embedded in smartphones, are widely used in our daily and corporate lives and contain the data of both employees and customers. With the growth of 5G networks, a new era of interconnection with IoT devices is emerging. The integration of 5G technology and IoT is set to expand the realm of fog computing, occupying the conceptual space between the cloud and edge computing. This is of significance, for example, for Industry 4.0 developments: the improvement in data processing speed and efficiency will bring cloud capabilities closer to where data is generated and analysis is performed, thus reducing latency and improving overall system performance [24]. This communication between multiple devices renders them open to security vulnerabilities from outside influences, attacks, or unknown software bugs. Effective management of such assets is a necessary aspect when considering cybersecurity culture [25].



Figure 2. The digital technologies (based on [26]).

Artificial intelligence (AI) and its deployment via machine learning have cross-company implications for cybersecurity. The recent emergence and rapidly expanding use of ChatGPT illustrates just how quickly and significantly AI technology can enter our daily lives [27]. It also provides an example of how digital technologies can be used to bypass the latest security protocols to create smart malware and control data to conduct cyberattacks. In the US, the National Institute of Science and Technology (NIST) has developed a framework to better manage risks associated with AI as regards individuals, organizations, and society. The NIST AI Risk Management Framework (AI RMF) aims to improve the integration of credibility concerns into the design, development, use, and evaluation of AI products, services, and systems [28]. Also, the EU AI Act is poised to be a pivotal piece of legislation, shaping the AI regulation landscape in the EU. As technology continues to evolve rapidly, concerns surrounding ethical AI development, data privacy, and algorithmic transparency have come to the fore. In this context, the EU AI Act purports to be a comprehensive framework designed to address these concerns, while fostering innovation and ensuring the responsible use of AI technologies [29].

Quantum computers will continue to evolve rapidly and facilitate high-level, complex computations that have new implications for IT governance [30]. This technology has a processing power that can solve many cryptographic algorithms by brute-force attack, especially in the short term. In the long run, however, quantum computers will likely make data more secure by enabling organizations investing in this space to reconsider existing encryption algorithms and processes [31].

Nevertheless, the net overall increase in potential cybersecurity threats resulting from rapid digitalization highlights the need for appropriate policies as well as skilled cybersecurity IT professionals within organizations [32]. From financial transactions to professional networking, organizations will increasingly use and rely upon digital technologies to support their business operations. Furthermore, since the COVID-19 pandemic, remote working has become significantly more important for businesses, but it has also introduced new cybersecurity risks that organizations must address [33]. Regulatory compliance is another key aspect of the challenge facing businesses, which must comply with a range of regulations and laws, including those concerning data privacy and the use of AI [34,35], some of which in-house IT departments may not be fully aware of [36].

3.2. *Strategy Alignment and Integration (Contextual Background)*

Organizations can more effectively recognize, evaluate, and control these risks by integrating their business, IT and cybersecurity strategies and plans. The benefits of effective business–IT strategy alignment are well documented, maximizing returns from IT investments and adding business value [37]. For example, research conducted by Poelen [38] on an SAP platform of a globally operating financial organization indicated that business–IT alignment had a positive effect on the business value of IT regarding communication, data sharing, and productivity (at local business unit level) and cost reduction (at central IT level). More specifically, Koçu [39] (p. 60) concluded that “business–IT alignment positively affects six dimensions of business agility: agile values, technology workforce, change management, collaboration and coordination, and flexible infrastructure”. On the other hand, a Harvard Business Review Analytic Services survey reported that lack of Business–IT alignment becomes a barrier to digital transformation, productivity, and value management [40]. However, the digital era has brought a new rationale for such alignment. The heightened risks associated with rapid digitalization, and ensuring the organization’s technology investments comply with the prevailing regulatory requirements, necessitate the alignment of business, IT and cybersecurity strategies.

In terms of how to approach this alignment, a number of models and frameworks have been put forward in recent decades. The Strategic Alignment Model (SAM) of Henderson and Venkatraman [41] is often seen as the standard from which several subsequent models and frameworks have been developed. There are two main dimensions—strategic fit and functional integration—in a four-quadrant model. A subsequent framework was developed by Aversano et al. [42] for measuring the degree of alignment between business processes and software systems, and de Castro et al. [43] developed a tool to analyse and enable alignment, using a Model Driven Architecture approach. The balanced scorecard [44] has also been used in this context. Bricknall et al. [45], for example, used the balanced scorecard to align IT strategy with business strategy in a pharmaceutical company, whilst Balafif and Haryanti [46] used an IT balanced scorecard for assessing the impacts of Business Strategy–IT alignment.

Building upon a number of these frameworks and models, Wynn and Weber [47] put forward a matrix model for strategy development and implementation, in which alignment of technology infrastructure, IT systems and business objectives was a key driver. It also suggested other frameworks and methods could operate under and within their umbrella model, including, for example, project management and IT Governance methods.

3.3. *IT Governance: The COBIT and the ISO 27000 Standards*

IT governance ensures compliance with laws and standards, and promotes a risk-based perspective, not ignoring the vulnerabilities that may arise from the use of technology. When the need for IT governance first emerged in the 1980s, there was no established

framework or method that organizations could use to manage their IT infrastructure. The ITIL (Information Technology Infrastructure Library) framework was then developed in the UK in the late 1980s, describing IT service management processes in detail and offering recommendations on how to design, plan, implement, operate, and continually improve these processes. ISACA (Information Systems Audit and Control Association) adapted ITIL's approach for IT service management to IT governance and released the COBIT (Control Objectives for Information and Related Technology) framework in 1996. In parallel, COSO (Committee of Sponsoring Organizations of the Treadway Commission) released an internal control and enterprise risk framework for corporate governance in 1992 [48]. In the first version of COBIT, an appropriate control framework for IT auditing was introduced based on COSO's internal control framework. In summary, COBIT is an IT governance framework that aligns information technology objectives with business objectives and processes by providing a risk perspective. COBIT provides customizable, comprehensive, and practical management to help organizations better manage their IT assets. COBIT 2019 consists of an extensive documentation set produced by ISACA, which covers governance and management objectives, design methodology, and implementation practices.

COBIT 2019: Governance and Management Objectives [2] and ISO/IEC 27014:2020 represent the most authoritative frameworks for IT governance and information security governance, respectively. As noted above, the COBIT 2019, the Governance and Management Objectives document details 40 governance and management objectives structured across five domains, including "Evaluate, Direct and Monitor" (EDM), "Align, Plan and Organize" (APO), "Build, Acquire and Implement" (BAI), "Deliver, Service and Support" (DSS), and "Monitor, Evaluate and Assess" (MEA). ISO/IEC 27014:2020 represents the core international standard specifically addressing the governance of information security. Its principles, processes, and role definitions provide a normative foundation for information security governance, making a comprehensive analysis both necessary and feasible. While COBIT 2019 offers updated guidance that reflects the latest trends and practices in IT governance, their predecessors COBIT 4.1 (dating from 2007) and COBIT 5 (dating from 2012) [49] remain important due to their established presence, familiarity, and alignment with existing organizational frameworks

In addition to ISO 27014, there are other standards of relevance that together provide a comprehensive framework for managing information security risks. ISO 27001, in particular, offers a standardized approach for implementing and managing information security management systems (ISMS). It requires organizations to identify, assess, and treat information security risks, ensuring a continuous improvement cycle. ISO 27005 [50] complements ISO 27001 by providing specific guidance on risk assessment and treatment. It outlines a systematic approach to risk management, from identification and assessment to treatment and monitoring. This standard helps organizations prioritize risks and allocate resources effectively. For organizations dealing with personal data, ISO 27701 offers valuable guidance on privacy management. It provides recommendations on how to identify, assess, and treat privacy risks, ensuring compliance with privacy laws and regulations like GDPR. This standard helps organizations protect sensitive information and maintain trust with their customers.

By adopting the ISO 27000 series of standards, organizations can potentially benefit in several regards. These include enhanced credibility, reduced risk of data breaches, improved operational efficiency, and enhanced compliance with industry-specific regulations. By following these standards, organizations can demonstrate their commitment to information security whilst protecting their valuable assets.

3.4. Provisional Conceptual Framework for Cybersecurity Strategy

A systematic analysis of the core governance framework (COBIT 2019) and security ISO/IEC 27000 series standards, as examined in Section 3.3, identified six critical themes for an integrated cybersecurity strategy, which also builds upon the emergent themes from the literature review. These six themes reflect the multi-dimensional risk landscape, including wider supply chain challenges. These are: IT Strategy and Digitalization; Cybersecurity Governance and Culture; Integrated Risk and Compliance Management; Performance Monitoring and Assurance; Strategic Alignment of Business, IT, and Security; and Stakeholder Engagement and Third-Party Risk (Figure 3).

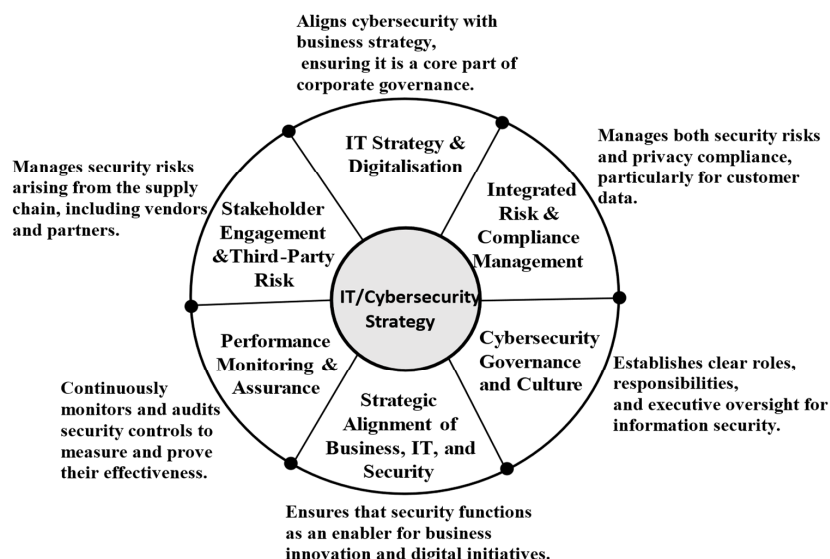


Figure 3. Provisional conceptual framework for cybersecurity strategy: six key themes (based on COBIT 2019 and ISO 27000 series standards).

The proposed framework integrates core principles from ISO/IEC 27001 (information security), ISO/IEC 27014 (governance), ISO/IEC 27701 (privacy), and ISO/IEC 27036 (supply chain security). To demonstrate the relevance of these themes and their traceability to the analyzed standards, the specific linkages to COBIT and ISO principles are mapped in Table 1.

Table 1. Provisional conceptual framework (PCF) themes: alignment and description.

PCF Themes	COBIT 2019 Basis	Aligned ISO 27000 Standards	Description/Key Activities
1. IT Strategy & Digitalization	APO02—Managed Strategy	ISO/IEC 27014:2020 (Clause 7.2.3—Set the direction of acquisition) Clause 7.3.3—Direct)	This theme addresses the dual opportunities and threats of digitalization (AI, IoT, etc.) discussed in Section 3.1. COBIT APO02 provides the IT strategy framework, while ISO 27014 guides the risk assessment of new technology adoption.
2. Cybersecurity Governance & Culture	EDM01—Ensured Governance Framework Setting and Maintenance	ISO/IEC 27014:2020 (Clause 7.2.1—Entity-wide governance; Clause 7.2.5—Security-positive culture)	COBIT provides the general IT governance structure, while ISO/IEC 27014 provides the specific information security governance principles, including the promotion of a “security-positive culture”.

Table 1. Cont.

PCF Themes	COBIT 2019 Basis	Aligned ISO 27000 Standards	Description/Key Activities
3. Integrated Risk & Compliance Management	EDM03—Ensured Risk Optimization APO12—Manage Risk MEA03—Managed Compliance with External Requirements	ISO/IEC 27014:2020 (Clause 7.2.2—Risk-based approach) ISO/IEC 27001 (Clause 6.1.2 risk assessment), Clause 6.1.3 (risk treatment) ISO/IEC 27701:2025 (PIMS)	This responds to the need to manage both security risks (ISO/IEC 27001/27014) and privacy/regulatory compliance (ISO/IEC 27701, GDPR) in a single, integrated framework.
4. Strategic Alignment of Business, IT, & Security	EDM02—Ensured Benefits Delivery	ISO/IEC 27014:2020 (Clause 7.2.6—Ensure the security performance meets current and future requirements of the entity) ISO/IEC 27001:2022 Clause 6.2 (Information security objectives)	The value of alignment is discussed in the extant literature (see Section 3.2). COBIT EDM02 links IT investments to business strategy. ISO/IEC 27014 explicitly links security performance to organizational performance.
5. Performance Monitoring & Assurance	MEA01—Managed Performance and Conformance Monitoring MEA02—Managed System of Internal Control MEA03—Managed Compliance with External Requirements	ISO/IEC 27014:2020 (Clause 7.3.4—Monitor) ISO/IEC 27001:2022 Clause 9 (Monitoring, measurement, analysis and evaluation), Clause 10 (Continual improvement)	There is a need to be able to measure the effectiveness of cybersecurity. This theme is derived from COBIT’s MEA (Monitor, Evaluate and Assess) domain, ISO/IEC 27014’s “Monitor” process, and ISO/IEC 27001’s clauses on performance evaluation.
6. Stakeholder Engagement & Third-Party Risk	EDM05— Ensured Stakeholder Engagement	ISO/IEC 27036 Series (Cybersecurity—Supplier relationships); ISO/IEC 27036-2:2022 (Requirements for supplier relationships); ISO/IEC 27036-3:2023 (Guidelines for hardware, software, and services for supply chain security); ISO/IEC 27014:2020 (Clause 7.3.5—Communicate).	This theme integrates COBIT’s focus on stakeholder Engagement with ISO/IEC 27014’s Clause 7.3.5 “Communicate” process and, critically, the specific third-party/supplier risk focus of the ISO 27036 series.

4. Results

4.1. RQ1. How Do COBIT and the ISO 27000 Series Standards Relate to Cybersecurity Issues?

This section addresses RQ1 using Qualitative Content Analysis as described in Section 2.1. In COBIT 2019 [2], cybersecurity strategy is not integrated within the broader framework of the governance and management of enterprise IT. The framework does not prescribe a specific cybersecurity strategy. Still, it suggests aligning cybersecurity with business objectives and ensuring it is managed effectively as part of the overall governance system. COBIT 2019 outlines 40 governance and management objectives and five domains that provide practical guidance for cybersecurity. Among these, EDM03: Ensure Risk Optimization is designed to help organizations identify, assess, and manage cybersecurity risks in alignment with their risk tolerance levels. At the same time, APO13: Manage Security supports the establishment and maintenance of strong information security and cybersecurity policies, processes, and controls to protect enterprise information and technology. Additionally, DSS05: Manage Security Services focuses on operationalizing the cybersecu-

urity strategy through the implementation of essential security services such as vulnerability management, incident response, and access controls. These objectives collectively guide organizations in building and maintaining effective cybersecurity practices.

However, they do not directly mention a cybersecurity strategy. This absence of a cybersecurity strategy framework can be addressed by the incorporation of ISO/IEC 27014, which provides guidance on the governance of information security, emphasizing that senior management should develop an information security strategy aligned with organizational objectives, ensuring that entity and information security requirements are harmonized to meet the current and evolving needs of stakeholders.

Key elements of COBIT and ISO/IEC 27014 can be mapped against the six themes established in the PCF as shown in Table 2, which consolidates the themes derived from the QCA. This analysis illustrates that while COBIT 2019 offers robust support for IT strategy formulation and governance, it does not specifically address cybersecurity strategy. ISO/IEC 27014 complements COBIT by providing governance principles that focus explicitly on information security (also known as cybersecurity), including risk-based decision-making, promoting a security culture, and enhancing stakeholder communication.

Table 2. COBIT and ISO/IEC 27014 references to PCF themes based on QCA.

Cybersecurity Strategy Theme/Code	COBIT 2019 Reference & Extract	ISO/IEC 27014:2020 Reference & Extract	Comment/Relevance
IT Strategy & Digitalization	APO02—Managed Strategy: “Provide a consistent approach integrated with enterprise strategy management to ensure IT enables and supports the achievement of enterprise objectives”.	7.2.3 Set the direction of acquisition: “The impact of information security risk should be adequately assessed when undertaking new activities, including adoption of new technology, outsourcing arrangements and contracts with external suppliers”.	Digitalization, AI, IoT, blockchain, metaverse as emerging risks/opportunities.
Cybersecurity Governance & Culture	COBIT covers IT governance broadly but is not a dedicated cybersecurity strategy. Example: EDM01—Ensured Governance Framework Setting and Maintenance: “Evaluate, direct and monitor the governance system and practices”.	7.2.1 Entity-wide governance: “Governance of information security should ensure that information security objectives are comprehensive and integrated at the entity level”. 7.3 Processes: “Evaluate, Direct, Monitor, Communicate”.	Developing a robust cybersecurity strategy; ISO fills COBIT’s gap at security governance level.
Risk & Compliance Integration	APO12—Managed Risk: “Establish and maintain a risk management framework that is integrated with enterprise risk management”. MEA03—Managed Compliance with External Requirements: “Evaluate adherence to laws, regulations and contractual requirements”.	7.2.2 Risk-based approach: “Governance of information security should be based on compliance obligations and risk-based decisions”. 7.2.4 Conformance: “Ensure that policies and practices conform to internal and external requirements”.	Compliance issues and IT security risks as central challenges.
Strategic Alignment of Business, IT & Security	EDM02—Ensured Benefits Delivery: “Ensure that IT-enabled investments deliver the expected benefits in line with business strategy”.	7.2.6 Ensure performance: “The governing body should link information security performance to the performance of the organization and of the entity”.	Alignment of business, IT, and cybersecurity strategies.

Table 2. Cont.

Cybersecurity Strategy Theme/Code	COBIT 2019 Reference & Extract	ISO/IEC 27014:2020 Reference & Extract	Comment/Relevance
Performance Monitoring & Assurance	MEA01— Managed Performance and Conformance Monitoring: “Collect, validate and evaluate business, IT and process goals and metrics”.	7.3.4 Monitor: “The governing body should receive the report on the effectiveness of the operation of each ISMS and evaluate it in the context of entity priorities”.	Framework usability is illustrated via an anonymised example, showing performance monitoring in practice.
Stakeholder Engagement & Third-party Risk	EDM05— Ensured Stakeholder Engagement: “Ensure that stakeholders are informed about the governance system’s performance and results”.	7.2.5 Security-positive culture: “Top management should require, promote and support coordination to establish a positive information security culture”. 7.3.5 Communicate: “Report to external interested parties that the entity practices a level of information security commensurate with the nature of its activities and priorities”.	Stakeholder engagement, user awareness, and cultural adaptation in digitalized environments.

A coherent cybersecurity strategy can be developed using the ISO standards in a layered approach: ISO/IEC 27014 provides the governance intent and direction at the top—clarifying the governing body’s role to evaluate, direct, monitor, and communicate so that security objectives are aligned with business goals and risk appetite (ISO/IEC 27014:2020). ISO/IEC 27001 operationalizes that intent through an ISMS: defining scope and context, establishing risk criteria, setting measurable security objectives, selecting and implementing controls, and running continuous Plan–Do–Check–Act improvement so strategy becomes an auditable management system (ISO/IEC 27001:2022). Finally, ISO/IEC 27036 broadens the strategy beyond the organization’s boundary by incorporating supplier and ICT supply chain security into sourcing and contracts. This requires the implementation of a supplier relationship strategy, risk-based acquisition decisions, assurance, performance monitoring, and cloud-specific responsibilities. where relevant (ISO/IEC 27036-1:2021; ISO/IEC 27036-2:2022; ISO/IEC 27036-3:2023; ISO/IEC 27036-4:2016). Together, 27014 (govern), 27001 (manage), and 27036 (extend to third parties) can translate leadership intent into enterprise-wide and supply chain-aware cybersecurity strategy, tightly coupled to business value, risk, compliance, and continuous improvement.

The directed QCA applied to ISO/IEC 27014:2020 and COBIT 2019 establishes traceability at both the clause and objective levels, providing the basis for evidence-based integration. It demonstrates how the governance intent of ISO/IEC 27014—encompassing Evaluate, Direct, Monitor, and Communicate, along with risk-based decision making, strategy approval, organizational culture, and stakeholder communication—correlates with COBIT’s governance mechanisms (Evaluate, Direct, and Monitor) and execution processes (Align, Plan, and Organize/Build, Acquire, and Implement/Deliver, Service, and Support). This mapping leads to the identification of the six strategic themes summarized in Table 2. Appendix B contains the codebook, examples, guidelines, and counts that support these themes.

4.2. RQ2. How Can These Standards Be Combined and Utilized in the Strategy Development Process?

The six strategy themes (Table 2) underpin a three-step development process, serving as design constraints and levers, and encompassing business, IT and cybersecurity strategies. These steps incorporate components of COBIT 2019, and the ISO/IEC 27000 series standards.

In Step 1 (Review & Align Business and IT Objectives), the themes frame board-level alignment: set or confirm measurable IS/IT objectives against enterprise goals (Strategic Alignment), define risk appetite and conformance expectations (Integrated Risk & Compliance), identify stakeholder/supplier expectations (Stakeholder & Third-Party), articulate cultural/role mandates (Governance & Culture), confirm digitalization priorities (IT Strategy & Digitalization), and agree performance indicators/review cadence (Performance & Assurance).

In Step 2 (Develop or Revise IT Strategy), each theme is translated into IT strategic choices and portfolios using COBIT 2019 governance/management objectives and practices (EDM/MEA for oversight; APO/BAI/DSS for plan-build-run)—e.g., APO02 for strategy, APO12 for risk, APO10/DSS with 27036 cues for suppliers, EDM01/EDM05 for governance and stakeholder Engagement, and MEA01–03 for performance and assurance.

In Step 3 (Define the Cybersecurity Strategy integrating COBIT 2019 and ISO/IEC 27000 series), the themes are instantiated as security objectives and controls using ISO/IEC 27014 for governance direction and ISO/IEC 27001 for ISMS objectives/risk treatment/controls, with ISO/IEC 27701 (privacy) and ISO/IEC 27036 (supplier) as contextual extensions; monitoring/communication obligations loop back into the performance and stakeholder themes. Thus, the themes are not labels but the operational backbone that drives Step 1 objectives, Step 2 IT strategy choices, and Step 3 cybersecurity strategy definition.

Building on the above process template, an exemplar case study was conducted to illustrate an integrated approach to cybersecurity strategy development, following this three-step process. This case study is an author-generated artefact and is for illustrative purposes only.

4.2.1. Step 1. Review and Align Business and IT Objectives

An essential building block for an effective cybersecurity strategy is the alignment of IT objectives with overall business strategy. This has been much discussed in business and IT literature [6,40–42,47] and is integral to COBIT 5 [49] and COBIT 2019 [2]. Table 3 presents an author-constructed analytical artifact derived from public sources and reported as an anonymized illustrative example.

Table 3. Alignment of business and IT objectives (illustrative example).

Business Objectives	IT Objectives
Increase system-wide sales by maintaining high digital penetration (70%+ of all orders) and growing online delivery share (currently 85% of delivery)	Ensure 99.9% uptime and sub-second response time for mobile/web ordering platforms during peak hours; scale Azure Kubernetes Service (AKS) infrastructure dynamically to handle traffic surges without degradation.
Maintain customer satisfaction through fast, reliable, and seamless digital experiences	Optimize end-to-end order fulfilment cycle time via real-time monitoring (Prometheus/Grafana/New Relic); reduce app crash rate to <0.1% and improve average page load time to under 1.5 s.

Table 3. Cont.

Business Objectives	IT Objectives
Ensure secure, compliant processing of payment transactions and customer data (PCI-DSS, privacy regulations)	Implement and maintain a formal Information Security Management System (ISMS) with annual third-party audits; enforce least-privilege access controls across all systems handling PII and payment data.
Support rapid product innovation and promotional agility (e.g., new menu launches, pricing experiments)	Enable CI/CD pipelines for zero-downtime deployment of new features and promotions; provide API-driven integration between CRM, POS, and marketing automation tools for targeted campaigns.
Optimize operational cost per order while scaling the store network (700+ locations)	Leverage cloud cost optimization tools (Azure Cost Management) to reduce infrastructure spend by 15% YoY; automate store-level technology provisioning via Infrastructure-as-Code (IaC).
Maintain executive and regulatory confidence as a publicly listed entity with significant third-party dependencies	Deliver quarterly cybersecurity risk reports to the Executive Committee; ensure documented SLAs and incident response coordination with the national managed services provider.

4.2.2. Step 2. Develop (or Revise) IT Strategy

Before considering a cybersecurity strategy per se, the existing IT strategy should be revisited and revised as necessary. COBIT 2019 (and previous COBIT versions) provide clear guidance on developing IT strategy, including APO02 (Figure 4).

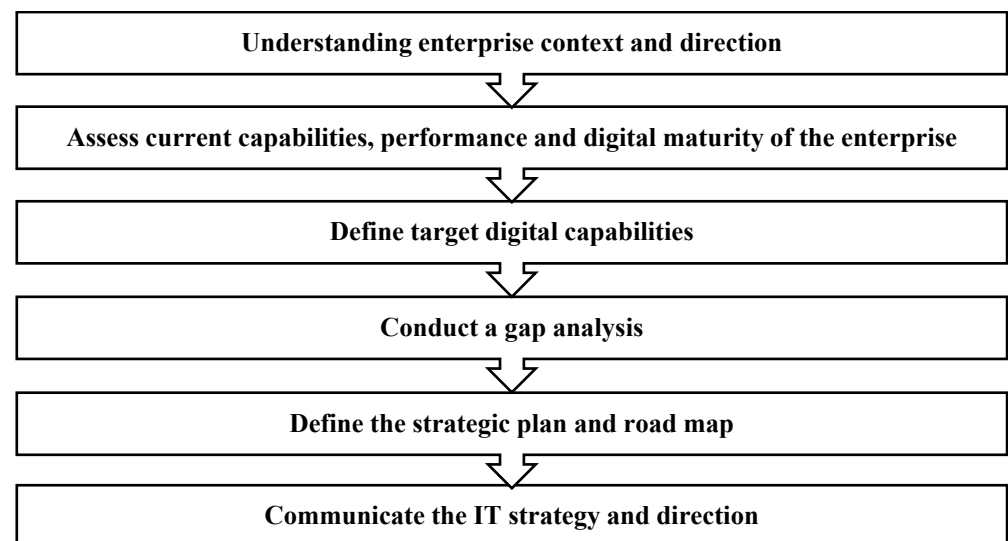


Figure 4. Defining an IT strategy in accordance with COBIT 2019 APO02 practices (top line).

Establishing an IT portfolio can be a useful approach in developing and aligning IT strategy. An IT portfolio can be seen as a set of managed technology assets, process investments, human capital assets, and project investments allocated to business strategies according to an optimal mix based on assumptions about future performance [51]. Managing the IT portfolio as a whole provides an effective way of ensuring technology investments are in line with overall business objectives. The company can make better choices about where to invest resources if it has a greater grasp of how technology supports

business goals. It offers a thorough overview of a company's technological architecture, making it easier to spot areas that require investment and set priorities for resources. A top-line example of IT strategy, based on the case study company, is provided in Appendix A, by way of illustration.

4.2.3. Step 3. Define the Cybersecurity Strategy Integrating COBIT 2019 and ISO/IEC 27000 Series

A cybersecurity strategy, aligned with IT and business strategies, should be sponsored by senior management and communicated between business, IT, and security staff. Upcoming changes, projects, challenges, and other concerns need regular review [52]. Table 4 extends the illustrative example contained in Table 3 to show alignment of business, IT, and cybersecurity objectives with initiatives/controls, ownership, and metrics for a cybersecurity strategy. This is an author-constructed analytical artifact, derived from public sources, of an anonymized exemplar company.

Table 4. Alignment of business, IT, and cybersecurity objectives with initiatives/controls, ownership, and metrics for cybersecurity strategy (illustrative example).

Business Objectives	IT Objectives	Cybersecurity Objectives	Key Initiatives/Control Sets (ISO Refs)	Accountable Owner & Timeline with KPI/KRI (MEA-Aligned)
Increase system-wide sales by maintaining high digital penetration (70%+ of all orders) and growing online delivery share (currently 85% of delivery)	Ensure 99.9% uptime and sub-second response time for mobile/web ordering platforms during peak hours; scale Azure Kubernetes Service (AKS) infrastructure dynamically to handle traffic surges without degradation.	Implement availability controls aligned with ISO/IEC 27001:2022 Clause 8.2 information security risk assessment. Ensure service continuity under load; embed DDoS protection and application-level WAF within AKS ingress to prevent disruption of revenue-generating channels.	High-availability architecture reviews; capacity/run-book tests; WAF & DDoS tuning; change gating for peak campaigns. ISO/IEC 27001 8.3; A.5.1, (info sec policy), A.8.6 (capacity management) A.5.30. (ICT readiness for business continuity)	CIO & CISO; Q2–Q3. KPI: % availability vs. SLA; failover MTTR. KRI: capacity breaches at peak. Review: MEA01.
Maintain customer satisfaction through fast, reliable, and seamless digital experiences	Optimize end-to-end order fulfillment cycle time via real-time monitoring (Prometheus/Grafana/New Relic); reduce app crash rate to <0.1% and improve average page load time to under 1.5 s.	Enforce secure software development lifecycle (SSDLC) practices to prevent vulnerabilities in user-facing applications; align with ISO/IEC 27001:2022 for secure development and testing.	Threat-model & SAST/DAST in pipeline; SBOM + dependency scanning; blue-green releases with rollback. ISO/IEC 27001 A.8.25 (Secure development life cycle), A.8.26 (Application security requirements), A.8.27 (Secure system architecture), A.8.28.(Secure coding), A.8.29 (Security testing in development)	Head of AppDev & CISO; Q2 pilot/Q3 rollout. KPI: % services with SSDLC gates; defect escape rate. KRI: P1 vulns age. Review: MEA01.

Table 4. Cont.

Business Objectives	IT Objectives	Cybersecurity Objectives	Key Initiatives/Control Sets (ISO Refs)	Accountable Owner & Timeline with KPI/KRI (MEA-Aligned)
Ensure secure, compliant processing of payment transactions and customer data (PCI-DSS, privacy regulations)	Implement and maintain a formal Information Security Management System (ISMS) with annual third-party audits; enforce least-privilege access controls across all systems handling PII and payment data.	Establish a Privacy Information Management System (PIMS) per ISO/IEC 27701:2025, ensuring lawful processing of customer data; integrate PCI-DSS controls into cloud architecture (e.g., tokenization, encryption at rest/in transit).	RoPA (Record of Processing Activities), DPIA (Data Privacy Impact Assessment) where needed; tokenisation and key management; PCI DSS attestation workflow; least-privilege enforcement. ISO/IEC 27701; ISO/IEC 27001 A.8.10-13 (information deletion, data masking, data leakage prevention, information backup); A.5.34 (privacy and protection of PII)	DPO & CISO; Q2 gap analysis/Q3 remediation. KPI: % systems with RoPA; % PCI controls passed. KRI: privacy incidents per 10k tx. Review: MEA03.
Support rapid product innovation and promotional agility (e.g., new menu launches, pricing experiments)	Enable CI/CD pipelines for zero-downtime deployment of new features and promotions; provide API-driven integration between CRM, POS, and marketing automation tools for targeted campaigns.	Apply security-by-design principles to DevOps pipelines; ensure automated vulnerability scanning and secrets management are integrated into CI/CD—supporting ISO/IEC 27001:2022 A.8.25-29 and 27014’s “integration with enterprise architecture”.	Automated Vulnerability scanning; secrets detection; container baseline hardening; feature-flag kill-switches. ISO/IEC 27001 A.8.25-29 (secure development life cycle, application security requirements, secure system architecture, secure coding, security testing in development)	DevOps Lead; Q2–Q4 phased. KPI: % pipelines with security gates; time-to-restore. KRI: leaked secret events. Review: MEA01.
Optimize operational cost per order while scaling the store network (700+ locations)	Leverage cloud cost optimization tools (Azure Cost Management) to reduce infrastructure spending by 15% YoY; automate store-level technology provisioning via Infrastructure-as-Code (IaC).	Implement cloud security posture management (CSPM) to detect misconfigurations that could lead to breaches or financial loss; align with ISO/IEC 27001:2022 Clause 8.2 information security risk assessment on asset management and protection.	CSPM policies (public storage, key rotation, MFA); asset inventory reconciliation; zero-trust network rules. ISO/IEC 27001 Clause 8.2 information security risk assessment—A5.23 (information security for use of cloud services)	Cloud CoE Lead; Q2 baseline/Q3 enforcement. KPI: % compliant resources; cost-avoidance. KRI: critical misconfig count. Review: MEA01.

Table 4. Cont.

Business Objectives	IT Objectives	Cybersecurity Objectives	Key Initiatives/Control Sets (ISO Refs)	Accountable Owner & Timeline with KPI/KRI (MEA-Aligned)
Maintain executive and regulatory confidence as a publicly listed entity with significant third-party dependencies	Deliver quarterly cybersecurity risk reports to the Executive Committee; ensure documented SLAs and incident response coordination with the national managed services provider.	Formalize third-party risk management per ISO/IEC 27036-3, including supplier agreements, continuous monitoring, and joint incident response plans; report security posture to board using ISO/IEC 27014:2020 Clause 7.3.4 (report on the effectiveness of the operation of each ISMS)	Supplier tiering; due diligence & contract clauses; continuous monitoring; incident notice terms. ISO/IEC 27036-2/-3; ISO/IEC 27014 Clause 7.3.5 Communicate. ISO/IEC 27001 A5.21-22 (managing information security in the ICT supply chain; monitoring, review and change management of supplier ser-vices)	Head of Procurement & Vendor Risk Manager with CISO; Q2 segmentation/Q3 contracts. Key Performance Indicator: % critical suppliers with 27036 clauses; % with evidence of controls. Key Risk Indicator: supplier non-conformities. Review: MEA03.

The six cybersecurity strategy themes can be applied across the three-step process to classify actions and ensure a comprehensive strategy outcome. An example is given in Table 5, illustrating the relevance of the ISO/IEC 27000 series standards, notably ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27036, and ISO/IEC 27014, as well as COBIT 2019.

Table 5. Mapping the six cybersecurity strategy themes to the three-step strategy development process with COBIT 2019 and ISO/IEC 27000 series integration.

Cybersecurity Strategy Themes	Step 1—Review & Align (Business–IT): key Actions	Step 2—Develop/Revise IT Strategy (via COBIT 2019)	Step 3—Define Cybersecurity Strategy (via ISO/IEC 27000)
Strategic Alignment of Business, IT & Security	Link IS/IT objectives to enterprise goals; define value targets	APO02 (Managed strategy), APO05 (Managed portfolio), APO06 (Managed Budget and Costs)	27014: Clause 7.3.3 Direct (approve IS strategy); 27001: Clause 6.2 Information Security objectives, Clause 5 Leadership, annex A (alignment controls)
Integrated Risk & Compliance Management	Set risk appetite/criteria; identify compliance obligations	APO12 (Managed risk), MEA03 (compliance), EDM03 (Ensured risk optimization)	27014: Clause 7.2.2 risk-based decisions; 27001: Clause 6.2/6.3 risk assessment/treatment plan; map key obligations
Performance Monitoring & Assurance	Choose KPIs/KRIs; review cadence; accountability	MEA01 (performance), MEA02 (Managed internal control), MEA03 (Managed Compliance with External Requirements)	27014: Clause 7.3.4 Monitor Clause 7.3.5 Communicate; 27001: Clause 9 (performance evaluation)
Cybersecurity Governance & Culture	Define “tone from the top”; roles/mandates; awareness goals	EDM01 (Ensured governance framework), APO07 (Managed Human Resource), APO08 (Managed relationships)	27014: Clause 7.2 governance objectives Inc. Clause 7.2.5 Foster a security-positive culture; 27001: Clause 7.2-7.4 (competence/awareness/communication)

Table 5. Cont.

Cybersecurity Strategy Themes	Step 1—Review & Align (Business–IT): key Actions	Step 2—Develop/Revise IT Strategy (via COBIT 2019)	Step 3—Define Cybersecurity Strategy (via ISO/IEC 27000)
IT Strategy & Digitalization	Prioritise digital adoption/retirement; sourcing choices	APO02 (managed strategy), BAI01 (Manage all programs from the investment portfolio in alignment with enterprise strategy), DSS01 (managed operations: coordinate and execute the activities and operational procedures required to deliver internal and outsourced I&T services), EDM04 (managed resource optimization)	27014: Clause 7.2.3 (direction of acquisition); 27001: Cloud & ICT Supply Chain controls (A.5.21, A.5.23)
Stakeholder Engagement & Third-Party Risk	Set expectations/outcomes for stakeholders and suppliers	EDM05 (stakeholder engagement), APO10 (managed vendors) DSS01-DSS04 (Deliver, Service and Support domain)	27014: report to interested parties; 27036: supplier governance; 27001: A.5.19-22 supplier controls

Figure 5 presents a practical governance model based on the findings from the QCA of COBIT 2019 and ISO/IEC 27014, as well as insights gained from the narrative synthesis of the mentioned standards. The ISO/IEC 27014 standard serves as the foundation for governance, guiding the board and top management in their directing, monitoring, and communication roles. COBIT 2019 specifies the execution of governance through defined objectives and practices, with EDM and MEA focusing on oversight, and APO, BAI, and DSS addressing planning, building, and operations. ISO/IEC 27001 establishes the Information Security Management System (ISMS) as the framework for setting objectives, managing risks, and implementing controls. Additionally, ISO/IEC 27701 integrates Privacy Information Management System (PIMS) requirements to ensure stakeholder privacy. Finally, ISO/IEC 27036 addresses external parties, with supplier risk recognized as an external factor managed through clear communication of expectations and relevant governance controls.

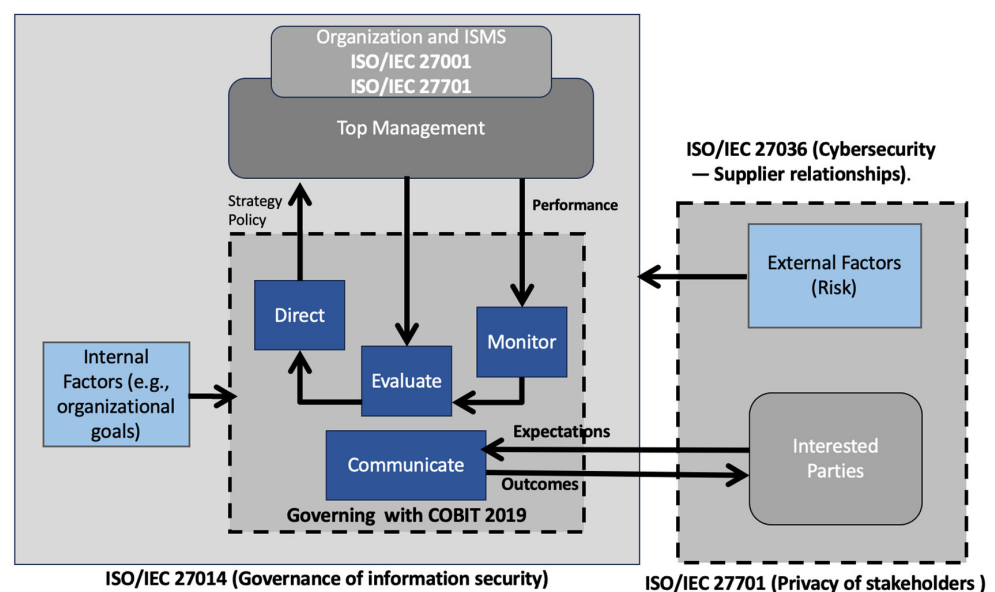


Figure 5. Integrated cybersecurity strategy governance model from QCA (ISO/IEC 27014 and COBIT 2019), with ISMS (ISO/IEC 27001), PIMS (ISO/IEC 27701) and supplier context (ISO/IEC 27036).

5. Discussion

The results presented above raise a number of issues worthy of brief discussion.

Firstly, the approach put forward here can be tailored to fit various regulatory and technological environments. ISO/IEC 27000 series of standards, like other ISO standards, is designed to be adaptable for organizations of all types and sizes. The derived framework based on the ISO/IEC 27000 series is further integrated with COBIT 2019, which provides mechanisms for execution and performance (including governance and management objectives, roles, practices, and monitoring for assurance). In addition, COBIT 2019 is specifically designed for tailored adoption through ISACA's design-factor guidance and supporting materials, which allows for applicability across various sectors, organizational sizes, and regulatory contexts, as long as it is customized to fit local objectives, risk appetite, sourcing models, and assurance requirements [53].

Secondly, there are a number of organizational change issues that need careful consideration and appropriate action. Implementing this framework may reveal resistance to change, gaps in skills and roles, and cultural frictions (such as low-risk ownership and compliance fatigue). To address these challenges, the integration incorporates (i) ISO/IEC 27001 risk assessment initiatives to promote a security-positive culture and ensure effective communication with stakeholders (including board-level sponsorship, clear accountability, and transparent reporting), and (ii) COBIT 2019 execution mechanics—APO07 for competencies and role design, BAI01/BAI05 for structured program/change enablement and stakeholder readiness, EDM01 for establishing and maintaining the governance framework and setting the “tone from the top”, and MEA01–03 for tracking performance, internal controls, and compliance. In practice, these measures should involve a skills uplift plan that includes training, hiring, and mentoring, as well as stakeholder mapping with a defined communication schedule. A phased rollout with early quick wins and indicators for culture and behavior (such as leadership messages, participation rates, and control adoption) should be reviewed in management and board meetings. These measures aim to reduce resistance, close capability gaps, and reinforce the culture needed for sustained execution.

Thirdly, the successful adoption of this approach requires a range of interrelated capabilities and processes to be in place across the organization. There must be committed senior management sponsorship, a programme to promote business understanding of the concepts and procedures involved at all levels, transparent and effective communication, and accurate inventories. The framework adds a structured governance layer that connects these factors to achieve measurable outcomes. The absence of any one of these building blocks may undermine this approach to cybersecurity strategy development and alignment with business and IT objectives.

6. Conclusions

The existing literature emphasizes the importance of aligning IT strategies with business processes and highlights the significance of cybersecurity strategies. However, there is a lack of comprehensive, step-by-step guidance on developing a cybersecurity strategy, which often leaves IT professionals unsure of where to start. This study has attempted to address that gap by putting forward a practical approach and associated guidelines.

The content analysis of COBIT 2019 and ISO/IEC 27014:2020 shows that these two frameworks provide complementary strengths for developing a robust cybersecurity strategy. COBIT offers a solid foundation for aligning IT strategy, performance monitoring, and integrating enterprise risk, but it does not address the specific requirements of cybersecurity governance. On the other hand, ISO/IEC 27014 explicitly focuses on information security governance by defining organization-wide objectives, risk-based decision-making processes, and mechanisms to promote a security-positive culture.

This complementarity is especially clear in areas such as strategic alignment, risk governance, compliance assurance, and stakeholder communication. COBIT provides the operational and managerial details, while ISO/IEC 27014 contributes the governance-level principles necessary to expand IT strategy into cybersecurity strategy. Together, the two standards enable organizations to align business, IT, and cybersecurity strategies, effectively bridging the gap between general IT governance and specific security governance.

The integrated framework promotes strategic alignment across business, IT, and cybersecurity by linking ISO/IEC 27014's governance objectives and processes to COBIT's EDM/MEA domains, facilitating execution through APO/BAI/DSS. The case example demonstrates its practicality as organizations can make risk-based decisions regarding emerging technologies (such as AI, blockchain, the metaverse, and decentralized finance), meet compliance obligations more effectively, and monitor security performance at the entity level—thus enhancing resilience, agility, and stakeholder trust. In the digital world driven by these new technologies, emerging threats such as market manipulation necessitate new capabilities, including real-time detection [54]. An effective cybersecurity strategy can protect organizations against such threats.

The study clearly has limitations. It is grounded in an analysis and application of existing standards and frameworks, and application of results requires a degree of top-down discipline and procedure that will not suit all company cultures. In addition, it includes a single exemplar case for illustration based on publicly available sources, but does not include interviews, reviews of internal documents, or any intervention or implementation by the authors. As a result, the findings support analytic generalization (as described by Yin [55]) related to feasibility and traceability, rather than providing insights into organizational adoption outcomes, and empirical validation was not conducted. Nevertheless, the authors believe the article provides both theoretical and practical contributions—a standards-aligned governance bridge from IT strategy to cybersecurity strategy and an outline guide that practitioners can adapt to specific business–IT environments. It is one of the first studies to integrate ISO/IEC 27014's board-level governance intent with COBIT 2019's governance/management mechanics using a directed QCA, yielding six strategy themes with clause/objective-level traceability. Future research could explore the framework across different industries and further develop the integration of COBIT and ISO standards in practical applications. Primary data, such as interviews, internal documents, and pre/post measures, could be used to assess implementation and its effects. Organizational pilots with expert validation via Delphi/focus groups and comparative studies would also be of value. Additionally, future studies could focus on the ongoing need to evolve cybersecurity strategies and methods in light of new technology developments, including the widening application of AI in the corporate environment and advent of the metaverse, which involves technologies and users operating in both physical and virtual spaces and will create new and different challenges for IT governance and cybersecurity [56]. This will only reinforce the need for strict alignment of business, IT and cybersecurity strategies within a rapidly evolving business and technology landscape.

Author Contributions: Conceptualization, B.M. and S.B.S.; methodology, B.M. and M.W.; validation, B.M. and M.W.; formal analysis, B.M. and S.B.S.; investigation, B.M. and S.B.S.; resources, S.B.S.; data curation, B.M. and S.B.S.; writing—original draft preparation, B.M. and M.W.; writing—review and editing, M.W.; visualization, B.M. and M.W.; supervision, B.M. and M.W.; project administration, B.M. and M.W.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Ethical review and approval were waived for this study because no human subjects were directly involved. There were no formal surveys or interviews involved in the data collection process.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data used in this study is available from the cited sources.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. Illustrative IT Strategy based on the Case Study company (key components; author-constructed, illustrative, anonymized, analytical artifact).

SECTION	CONTENT
OVERVIEW	The IT function enables the company's digital-first, customer-centric strategy through scalable cloud infrastructure, real-time data analytics, and secure, agile delivery platforms.
MISSION STATEMENT	To deliver reliable, innovative, and secure technology solutions that support rapid growth, operational efficiency, and exceptional customer experiences across 700+ locations in Turkey.
OBJECTIVES	<ul style="list-style-type: none"> • Ensure 99.9% uptime for digital ordering platforms (mobile/web). • Reduce cost per order by 10% via automation and cloud optimization. • Maintain PCI-DSS and privacy compliance across all systems handling PII and payment data. • Enable rapid product innovation through CI/CD pipelines and API-driven architecture.
ASSESSMENT/AUDIT	Current state: Hybrid model with internal strategic IT team (30–35 FTEs) and external managed services partner for infrastructure (Azure AKS, monitoring, DevOps).
INVENTORY—CLOUD & INFRASTRUCTURE	<ul style="list-style-type: none"> • Azure Kubernetes Service (AKS). • Azure App Services, Blob Storage, SQL DB. • Prometheus, Grafana, Alertmanager (monitoring). • New Relic (application performance). • Global peering between legacy App Services and AKS.
INVENTORY—APPLICATIONS & PLATFORMS	<ul style="list-style-type: none"> • Web applications, mobile app (iOS/Android). • CRM & loyalty platform. • POS integration system. • Aggregator APIs (Trendyol Go by Uber Eats, Getir Yemek, Yemeksepeti). • Franchisee portal & reporting dashboard.
NETWORK COMPONENTS	<ul style="list-style-type: none"> • Secure API gateway. • WAF (Web Application Firewall). • Zero-trust network access for remote teams. • DDoS protection layer.
PLAN—STRATEGIC ACTIONS	<ol style="list-style-type: none"> 1. Implement ISO/IEC 27001 ISMS and 27701 PIMS for formal security & privacy governance. 2. Automate deployment pipelines using GitOps principles on AKS. 3. Enhance real-time fraud detection and anomaly monitoring via ML models. 4. Establish third-party risk management framework aligned with ISO/IEC 27036.
PROJECT BUDGET	<ul style="list-style-type: none"> • 60% infrastructure & cloud costs. • 25% application development & maintenance. • 10% cybersecurity & compliance. • 5% training & innovation R&D.

Table A1. Cont.

SECTION	CONTENT
DEPARTMENT STRUCTURE	<ul style="list-style-type: none"> • Application Development (12–15). • Cloud & Infrastructure (6–8). • Cybersecurity & Compliance (3–5). • Data & Analytics (4–6). • IT Support & Operations (3–4). • External Partner Management (managed services provider).
APPROVAL DATE BY SENIOR MANAGEMENT	Q1 2025

Appendix B. Qualitative Content Analysis Illustrative Documents

Table A2. Coding frame with definitions and decision rules.

Code	Definition (What It Captures)	Inclusion Rules (Code When...)	Exclusion Rules (Do Not Code When...)	Typical Indicators in the Coded Corpus
IT Strategy & Digitalization	Direction for adopting/retiring technologies (AI, IoT, cloud, etc.) and linking such decisions to governance and risk.	Mentions acquisition/adoption direction, governance criteria for new tech, or risk-aware selection/outsourcing.	Pure technical features or tool lists without governance direction.	27014: “set the direction of acquisition”; COBIT: APO02 Manage Strategy.
Cybersecurity Governance & Culture	Security-specific governance principles and fostering a security-positive culture led by top management/board.	Mentions security governance principles, roles/mandates, tone-from-the-top, culture/awareness.	Control configuration or training logistics without governance/culture intent.	27014: entity-wide governance; security-positive culture. COBIT: EDM01.
Integrated Risk & Compliance Management	Risk-based decision-making at entity level and conformance/assurance integration (including privacy where relevant).	Mentions risk appetite/criteria, ERM integration, conformance/assurance planning or evidence requirements.	Isolated operational risks or checklists without governance of risk/conformance.	27014: risk-based approach; conformance/assurance. COBIT: APO12; MEA03.
Strategic Alignment of Business, IT, & Security	Linking IS/IT objectives and benefits to enterprise goals; governance approval of strategy and measurable objectives.	Mentions alignment with business strategy, benefits delivery, measurable IS objectives, architecture fit.	Technology selection without business linkage or metrics.	27014: ensure performance; evaluate/direct strategy. COBIT: EDM02.
Performance Monitoring & Assurance	Setting indicators/targets, monitoring/reviewing security performance, and assurance over controls.	Mentions KPIs/KRIs, dashboards, management review cadence, audit/assurance.	One-off testing with no linkage to performance or governance review.	27014: “Monitor” process; COBIT: MEA01–MEA03.
Stakeholder Engagement & Third-Party Risk	Bi-directional communication with interested parties and governance of supplier/third-party risks.	Mentions reporting to stakeholders, expectations/outcomes, supplier requirements/assurance.	Internal team comms only; vendor how-to without governance requirements.	27014: “Communicate” to interested parties; COBIT: EDM05; (contextual link to 27036 in discussion, not coded).

Coding policy: Single primary code per segment; allow one optional secondary code when the segment genuinely spans two governance intents (mark as “secondary”).

Table A3. Examples of coded text segments.

Source	Short Excerpt (≤ 25 Words, Verbatim)	Assigned Code	Rationale (Why This Code/Strategy Relevance)
ISO/IEC 27014:2020, 7.2.3	“Set the direction of acquisition. . .”	IT Strategy & Digitalization	Ties adoption/outsourcing choices to governance criteria; mandates risk-aware strategic direction for AI/IoT/cloud decisions.
COBIT 2019, APO02 (purpose)	“Manage I&T strategy to support enterprise strategy and goals.”	IT Strategy & Digitalization	Frames I&T strategy as subordinate to business goals; ensures digital initiatives are governed for contribution and measurable outcomes.
ISO/IEC 27014:2020, 7.2.1	“Information security objectives should be related to. . . the overall goals of the entity.”	Strategic Alignment of Business, IT, & Security	Forces explicit linkage of IS objectives to enterprise goals—alignment, value, and performance orientation.
COBIT 2019, EDM02 (purpose)	“Ensure benefits delivery from I&T-enabled investments.”	Strategic Alignment of Business, IT, & Security	Board-level accountability for benefits realisation; governance mechanism to track value and maintain alignment.
ISO/IEC 27014:2020, 7.2.2	“Make decisions using a risk-based approach.”	Integrated Risk & Compliance Management	Entity-level mandate to apply risk appetite/criteria; integrates compliance/assurance expectations into decision-making.
COBIT 2019, APO12 (purpose)	“Manage I&T-related risk in line with enterprise risk management.”	Integrated Risk & Compliance Management	Integrates I&T risk with ERM; clarifies ownership, reporting, and control design under governance.
ISO/IEC 27014:2020, 7.3.4	“Monitor performance of information security. . .”	Performance Monitoring & Assurance	Requires KPIs/KRIs and management review; establishes governance expectations for performance oversight.
COBIT 2019, MEA01 (purpose)	“Collect, validate and evaluate business, I&T and process goals and metrics.”	Performance Monitoring & Assurance	Sets a full metrics cycle—collection, validation, evaluation—and links to corrective actions and assurance.
ISO/IEC 27014:2020, 7.2.5	“Foster a security-positive culture.”	Cybersecurity Governance & Culture	Elevates culture to a governance objective; assigns top-management responsibility for roles, awareness, competence.
COBIT 2019, EDM01 (purpose)	“Ensure governance framework setting and maintenance.”	Cybersecurity Governance & Culture	Establishes and maintains the enterprise governance framework—structure to manage culture and roles systematically.
ISO/IEC 27014:2020, 7.3.5	“Report to interested parties. . .”	Stakeholder Engagement & Third-Party Risk	Mandates bidirectional reporting to stakeholders; strengthens accountability and transparency of security outcomes.
COBIT 2019, EDM05 (purpose)	“Ensure stakeholder Engagement for I&T governance.”	Stakeholder Engagement & Third-Party Risk	Requires stakeholder Engagement; frames expectation/outcome reporting, relevant to supplier/third-party contexts.

Table A4. Coding rules and decision protocol.

Rule	Description
Segmentation	ISO/IEC 27014 coded at clause/paragraph level; COBIT 2019 coded at objective “purpose” and management practice paragraph level.
Primary vs. secondary codes	Assign exactly one primary code per segment; add one secondary only if the text genuinely reflects two governance intents.
Ambiguity rule	If a segment fits both alignment and performance, prefer Strategic Alignment when it prescribes direction/objectives; prefer Performance Monitoring & Assurance when it prescribes measurement/review mechanics.
Negative evidence	If a segment states absence/shortcomings (e.g., “lack of metrics”), still code under the intended category and flag as NEG.
Memoing	Record coder notes and any inductive sub-codes in a shared log (date, coder, rationale).
Adjudication	Resolve disagreements by consensus; if unresolved, the senior coder adjudicates. Maintain version control for changes.

As a single-coder study, trustworthiness was ensured via an auditable memo trail, peer debriefing, negative-case logging, and version control.

Table A5. Evidence of systematic application (counts).

Code (Theme)—	Segments Coded (COBIT 2019)	Segments Coded (ISO/IEC 27014)	Total
IT Strategy & Digitalization	2	1	3
Cybersecurity Governance & Culture	2	1	3
Integrated Risk & Compliance Management	2	2	4
Performance Monitoring & Assurance	3	2	5
Strategic Alignment of Business, IT, & Security	1	2	3
Stakeholder Engagement & Third-Party Risk	2	2	4
Total	12	10	22

References

- Gill, O.; Yorke, H. £1.5bn Rescue to Keep Wheels Turning Till Christmas at Hacked JLR and Suppliers. *Sunday Times* **2025**, *489*, 2.
- ISACA. *COBIT 2019 Framework: Governance & Management Objectives*; ISACA: Schaumburg, IL, USA, 2018. Available online: <https://www.isaca.org/resources/cobit> (accessed on 5 June 2025).
- Slim, A.; Sarah, O.; Kadhim, K.; Ali, B.; Hammood, A.; Othman, B. The effect of information technology business alignment factors on performance of SMEs. *Manag. Sci. Lett.* **2021**, *11*, 833–842. [[CrossRef](#)]
- Adaba, G.B.; Wilson, D.W.; Sims, J. The Impact of National Culture on Strategic IT Alignment: A Multiple-case Study of Subsidiaries of Multinational Corporations. *Inf. Syst. Manag.* **2022**, *39*, 288–304. [[CrossRef](#)]

5. Alaceva, C.; Rusu, L. Barriers in achieving business/IT alignment in a large Swedish company: What we have learned? *Comput. Hum. Behav.* **2015**, *51*, 715–728. [CrossRef]
6. Earl, M. *Management Strategies for Information Technology*; Prentice Hall: Hemel Hempstead, UK, 1989.
7. Sayjari, T.; Melo Silveira, R. Cybersecurity and Corporate Risk Management: Aligning Information Security with Business Strategies. In Proceedings of the Congresso de Gestão de Riscos Corporativos (GRC), São Paulo, Brazil, December 2024.
8. ISO/IEC 27000; Family—Information Security Management. ISO. Available online: <https://www.iso.org/standard/iso-iec-27000-family#:text=IT%20security%2C%20cybersecurity%20and%20privacy,information%20entrusted%20by%20third%20parties> (accessed on 12 November 2025).
9. ISO/IEC 27014; Information Security, Cybersecurity and Privacy Protection—Governance of Information Security (ISO/IEC Standard No. 27014:2020). ISO/IEC: Geneva, Switzerland, 2020. Available online: <https://www.iso.org/standard/74046.html> (accessed on 23 July 2025).
10. ISO/IEC 27001; Information Security, Cybersecurity, and Privacy Protection—Information Security Management Systems—Requirements (ISO/IEC Standard No. 27001:2022). ISO/IEC: Geneva, Switzerland, 2022. Available online: <https://www.iso.org/standard/82875.html> (accessed on 15 May 2025).
11. ISO/IEC 27036; ISO/IEC 27036-1:2021 Cybersecurity—Supplier Relationships—Part 1: Overview and Concepts. ISO/IEC: Geneva, Switzerland, 2021. Available online: <https://www.iso.org/standard/82905.html> (accessed on 8 May 2025).
12. ISO/IEC 27036-2; ISO/IEC 27036-2:2022 Cybersecurity—Supplier Relationships—Part 2: Requirements. ISO/IEC: Geneva, Switzerland, 2022. Available online: <https://www.iso.org/standard/82060.html> (accessed on 8 May 2025).
13. ISO/IEC 27036-3; ISO/IEC 27036-3:2023 Cybersecurity—Supplier Relationships—Part 3: Guidelines for hardware, software, and services supply chain security. ISO/IEC: Geneva, Switzerland, 2023. Available online: <https://www.iso.org/standard/82890.html> (accessed on 8 May 2025).
14. ISO/IEC 27036-4; ISO/IEC 27036-4:2016 Information Technology—Security Techniques—Information Security for Supplier Relationships—Part 4: Guidelines for Security of Cloud Services. ISO/IEC: Geneva, Switzerland, 2016. Available online: <https://www.iso.org/standard/59689.html> (accessed on 13 October 2025).
15. ISO/IEC 27701:2025; Information Security, Cybersecurity and Privacy Protection—Privacy Information Management Systems—Requirements and Guidance (2nd ed.). Available online: <https://www.iso.org/standard/27701> (accessed on 2 November 2025).
16. Snyder, H. Literature review as a research methodology: An overview and guidelines. *J. Bus. Res.* **2019**, *104*, 333–339. [CrossRef]
17. Webster, J.; Watson, R.T. Analyzing the past to prepare for the future: Writing a literature review. *MIS Q.* **2002**, *26*, xiii–xxiii.
18. Popay, J.; Roberts, H.; Sowden, A.; Petticrew, M.; Arai, L.; Rodgers, M.; Britten, N.; Roen, K. Guidance on the conduct of narrative synthesis in systematic reviews. *ESRC Methods Programme* **2006**, *1*, b92.
19. Petticrew, M.; Roberts, H. *Systematic Reviews in the Social Sciences: A Practical Guide*; Blackwell Publishing: Oxford, UK, 2006.
20. Mayring, P. Qualitative Content Analysis. *Forum Qual.* **2000**, *1*, 20. Available online: <https://www.qualitative-research.net/index.php/fqs/article/view/1089/2385> (accessed on 3 October 2025).
21. Schreier, M. *Qualitative Content Analysis in Practice*; Sage: London, UK, 2012.
22. Wynn, M.; Bakeer, A.; Forti, Y. E-government and digital transformation in Libyan local authorities. *Int. J. Teach. Case Stud.* **2021**, *12*, 119–139. [CrossRef]
23. Taylor, J.; Wynn, M. Case study methodologies and a wider appreciation of development planning. *Ekistics* **1980**, *47*, 451–453. Available online: <https://eprints.glos.ac.uk/8716/> (accessed on 3 October 2025).
24. Mutlutürk, M.; Kor, B.; Metin, B. *The Role of Edge/Fog Computing Security in IoT and Industry 4.0 Infrastructures: Edge/Fog-Based Security in Internet of Things*; IGI Global: Hershey, PA, USA, 2021; pp. 211–222. ISBN 13: 9781799877400. [CrossRef]
25. Metin, B.; Duran, S.; Telli, E.; Mutlutürk, M.; Wynn, M. IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation that Engenders a Security Culture. *Information* **2024**, *15*, 55. [CrossRef]
26. Wynn, M. E-business, Information Systems Management and Sustainable Strategy Development in the Digital Era. *Sustainability* **2022**, *14*, 10918. [CrossRef]
27. Roose, K. The Brilliance and Weirdness of ChatGPT. *The New York Times*. 9 December 2022. Available online: <https://www.nytimes.com/2022/12/05/technology/chatgpt-ai-twitter.html> (accessed on 10 October 2024).
28. NIST Information Technology Laboratory. *AI Risk Management Framework by NIST*; NIST Information Technology Laboratory: Gaithersburg, MD, USA, 2023. Available online: <https://www.nist.gov/itl/ai-risk-management-framework> (accessed on 2 October 2025).
29. Laux, J.; Wachter, S.; Mittelstadt, B. Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk. *Regul. Gov.* **2024**, *18*, 3–32. [CrossRef]
30. Wynn, M.; Jones, P. Corporate Digital Responsibility and the Business Implications of Quantum Computing. *Adv. Environ. Eng. Res.* **2023**, *4*, 1–18. [CrossRef]
31. Cherbal, S.; Zier, A.; Hebal, S.; Louail, L.; Annane, B. Security in internet of things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing. *J. Supercomput.* **2024**, *80*, 3738–3816. [CrossRef]

32. Goulart, V.G.; Liboni, L.B.; Cezarino, L.O. Balancing skills in the digital transformation era: The future of jobs and the role of higher education. *Ind. High. Educ.* **2022**, *36*, 118–127. [CrossRef]
33. Tanriverdi, N.S.; Metin, B. *Enterprise Information Security Awareness and Behavior as An Element of Security Culture During Remote Work: Security Awareness and Behavior During Remote Work*; IGI Global: Hershey, PA, USA, 2021; pp. 119–138, ISBN 13: 9781799875130. [CrossRef]
34. Sebastian, G. Privacy and Data Protection in ChatGPT and Other AI Chatbots: Strategies for Securing User Information. *International. J. Secur. Priv. Pervasive Comput.* **2023**, *15*, 1–14. [CrossRef]
35. Jessani, A. *Chatbots, AI and the Future of Privacy*; IAPP: Portsmouth, NH, USA, 23 March 2023. Available online: <https://iapp.org/news/a/chatbots-ai-and-the-future-of-privacy/> (accessed on 18 May 2025).
36. Tom, J.; Adigwe, W.; Anebo, N.; Bukola, O. Automated Model for Data Protection Regulation Compliance Monitoring and Enforcement. *Int. J. Comput. Intell. Secur. Res.* **2023**, *2*, 47–57.
37. Elmorshidy, A. Aligning IT With Business Objectives: A Critical Survival and Success Factor in today’s Business. *J. Appl. Bus. Res.* **2013**, *29*, 819–828. [CrossRef]
38. Poelen, E. The Implications of Business-IT Alignment for Business Value of IT. 8 May 2017. Available online: <http://arno.uvt.nl/show.cgi?fid=144854> (accessed on 8 May 2025).
39. Koçu, L. Business -IT alignment effects on business agility. *Int. J. Commer. Financ.* **2018**, *4*, 60–93.
40. Broadcom. Is Your IT Department Aligned with Your Business Outcomes? 1 September 2020. Available online: <https://hbr.org/sponsored/2020/09/is-your-it-department-aligned-with-your-business-outcomes> (accessed on 3 October 2025).
41. Henderson, J.C.; Venkatraman, N. Strategic Alignment: Leveraging Information Technology for Transforming Organizations. *IBM Syst. J.* **1993**, *32*, 4–16. [CrossRef]
42. Aversano, L.; Grasso, C.; Tortorella, M. Measuring the Alignment Between Business Processes and Software Systems: A Case Study. In Proceedings of the 2010 ACM Symposium on Applied Computing (SAC’10), Sierre, Switzerland, 22–26 March 2010.
43. De Castro, V.; Marcos, E.; Vara, J.M. Applying CIM-to-PIM model transformations for the service-oriented development of information systems. *J. Inf. Softw. Technol.* **2011**, *53*, 87–105. [CrossRef]
44. Kaplan, R.S.; Norton, D.P. *Balanced Scorecard: Implementing and Action Strategy*; Erlangga: Jakarta, Indonesia, 2000.
45. Bricknall, R.; Darrell, G.; Nilsson, H.; Pessi, K. Aligning IT strategy with business strategy through the balanced scorecard in a multinational pharmaceutical company. In Proceedings of the 2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07), Waikoloa, HI, USA, 3–6 January 2007.
46. Balafif, S.; Haryanti, T. IT balanced scorecard (IT BSC) based strategic framework for assessing the impacts of Business Strategic-IT alignment. *IOP Conference Series. Mater. Sci. Eng.* **2020**, *821*, 12033. [CrossRef]
47. Wynn, M.; Weber, C. Information Systems Strategy for Multi-National Corporations: Towards an Operational Model and Action List. *Information* **2024**, *15*, 119. [CrossRef]
48. COSO. *Committee of Sponsoring Organizations of the Treadway Commission, Internal Control—Integrated Framework: Executive Summary*; COSO: New York, NY, USA, 1992.
49. ISACA. *Transforming Cybersecurity Using COBIT5*; ISACA: Schaumburg, IL, USA, 2013; ISBN 978-1-60420-341-7. Available online: <https://www.isaca.org/> (accessed on 12 May 2025).
50. ISO/IEC 27005:2022; Information Security, Cybersecurity and Privacy Protection—Guidance on Managing Information Security Risks. ISO/IEC: Geneva, Switzerland, 2022. Available online: <https://www.iso.org/standard/80585.html> (accessed on 12 September 2025).
51. Cameron, B.H. IT Portfolio Management: Implications for IT Strategic Alignment. In Proceedings of the Eleventh Americas Conference on Information Systems, Omaha, NE, USA, 11–14 August 2005.
52. Violino, B. How to Better Integrate IT Security and IT Strategy. 2019. Available online: <https://www.cio.com/article/3407737/how-to-better-integrate-it-security-and-it-strategy.html> (accessed on 23 August 2025).
53. ISACA. *Designing Your Organization’s Custom COBIT*; ISACA: Schaumburg, IL, USA, 2019; Available online: <https://www.isaca.org/resources/news-and-trends/industry-news/2019/designing-your-organizations-custom-cobit> (accessed on 25 October 2025).
54. Wu, C.; Chen, J.; Li, J.; Xu, J.; Jia, J.; Hu, Y.; Feng, Y.; Liu, Y.; Xiang, Y. Profit or Deceit? Mitigating Pump and Dump in DeFi via Graph and Contrastive Learning. *IEEE Trans. Inf. Forensics Secur.* **2025**, *20*, 8994–9008. [CrossRef]
55. Yin, R.K. *Case Study Research and Applications: Design and Methods*, 6th ed.; Sage: Thousand Oaks, CA, USA, 2018.
56. Wynn, M.; Jones, P. New technology deployment and corporate responsibilities in the metaverse. *Knowledge* **2023**, *3*, 543–556. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.