

Cybersecurity Governance and Data Protection in Digital Transactions: A Comparative Legal Analysis of Saudi Regulations and International Frameworks

DR. YUSSRI AWAD ABDALLA

Director of the Legal Department, Al Fozan Holding Group. AL Khobar, Kingdom of Saudi Arabia.
E-Mail: dr.yussri.a.abdullah@gmail.com <https://orcid.org/0009-0005-4853-732X>

Abstract: This study examines the legal and regulatory framework governing cybersecurity governance and data protection in digital transactions through an analytical and comparative assessment of Saudi regulations against relevant international frameworks and standards. It assesses how effectively the Saudi regulatory environment integrates a governance model based on international best practices to enhance digital trust and the security of digital transactions. The research adopts a doctrinal legal research design based on analytical and comparative approaches to examine Saudi laws, regulations, and cybersecurity controls, combined with a comparative approach to evaluate their consistency with leading international references, particularly the NIST Cybersecurity Framework (CSF 2.0), ISO/IEC 27001, ISO/IEC 27701, and the European Union General Data Protection Regulation (GDPR). The study concludes that the Saudi regulatory framework provides an advanced governance model that integrates institutional governance, cybersecurity risk management, regulatory compliance, data protection, and business continuity, reflecting substantial alignment with contemporary international standards. Securing digital transactions depends on the integration of governance, risk management, operational controls, audit, and regulatory frameworks rather than purely on legislative and technological approaches. The study contributes to the legal scholarship by developing an integrated analytical framework that combines cybersecurity governance, data protection, and digital transactions from a regulatory perspective. It also offers comparative insights for policymakers, regulators, and firms that want to enhance digital trust and promote the sustainable growth of the digital economy in Saudi Arabia.

Keywords: Cybersecurity governance; data protection; digital transactions; cyber risk management; Saudi Arabia; regulatory framework; digital trust

1. Introduction

The world has witnessed, over the past two decades, a radical transformation in legal and economic transactions as a result of the digital revolution, which has reshaped the patterns of interaction among individuals, institutions, and states. Commercial, financial, and administrative transactions no longer rely on traditional means, but increasingly depend on digital platforms, cloud services, artificial intelligence, blockchain, financial technology (FinTech), digital identity technologies, electronic signatures, and electronic payment systems, giving rise to what has come to be known as the digital economy, in which data has become the most valuable resource, and digital trust has become the essential pillar for the stability and continuity of transactions.

This transformation has contributed to significant economic and legal advantages, manifested in accelerating the completion of transactions, reducing operating costs, expanding the scope of trade and investment, enhancing financial inclusion, and improving the efficiency of government and private services. It has, however, at the same time created a highly complex digital environment in which cyber risks are increasing at an accelerating pace, and these



risks have become one of the most significant challenges facing the global digital economy, as cyberattacks have shifted from limited individual acts into organized, cross-border operations targeting critical infrastructure, the financial sector, capital markets, e-commerce platforms, cloud-computing service providers, government databases, and data-processing centers, thereby threatening the confidentiality, integrity, and availability of data, the three principles on which information security and cybersecurity are founded across all international frameworks (ISO/IEC 27001; NIST CSF2.0).

In contemporary legal thought, cybersecurity is no longer merely a technical system aimed at protecting networks, devices, and software; it has become one of the elements of institutional governance, a principal tool for risk management, a means of ensuring legislative compliance, protecting digital rights and freedoms, and preserving trust in the digital environment. Cybersecurity has accordingly moved from being a technical function undertaken by information-technology departments to being a strategic responsibility resting with boards of directors, executive management, and regulatory bodies, and one of the most important indicators of sound governance and business sustainability (National Institute of Standards and Technology [NIST], 2024).

This transformation takes on even greater importance where digital transactions are concerned, since the success and stability of such transactions rest on trust in the safety of the electronic environment through which they take place. The higher the level of cybersecurity protection, the greater the trust of individuals and institutions in using digital means, and vice versa; any breach, data leak, or system disruption may give rise to far-reaching legal and economic consequences, including loss of trust, business disruption, civil liability, and regulatory penalties, in addition to direct and indirect financial losses.

Accordingly, the majority of states have moved toward building integrated legislative and regulatory systems to protect the digital environment, such that legal texts are no longer confined to criminalizing attacks on information systems, but have extended to regulating cybersecurity governance, risk management, personal data protection, requiring establishments to apply protective controls, establishing policies for disclosing cyber incidents, regulating the responsibilities of boards of directors and executive management, and establishing principles of compliance, oversight, and auditing, achieving integration between legal and technical protection.

In the Kingdom of Saudi Arabia, this development has been consistent with the objectives of Saudi Vision 2030, which has made digital transformation one of the most important drivers of economic development. The regulatory environment has accordingly witnessed the issuance of several laws and controls which, taken together, form an integrated framework for cybersecurity governance and data protection, most notably the Electronic Transactions Law, the Anti-Cyber Crime Law, the E-Commerce Law, the Personal Data Protection Law, and the Essential Cybersecurity Controls issued by the National Cybersecurity Authority, alongside the regulatory frameworks issued by the Saudi Central Bank and the Capital Market Authority, which have not been confined to setting technical protection requirements but have linked cybersecurity to institutional governance, risk management, business continuity, customer protection, incident reporting, vendor management, and continuous auditing. Saudi regulatory guides confirm that responsibility for cybersecurity begins with the board of directors and extends to all levels of the institution, with an emphasis on governance, risk management, operational controls, third parties, and business continuity.

The international arena, for its part, has witnessed notable development in building normative frameworks regulating cybersecurity, foremost among them the NIST CSF 2.0, ISO/IEC 27001 and ISO/IEC 27701, the European Union General Data Protection Regulation (GDPR), and the Budapest Convention on Cybercrime, frameworks that no longer focus on the technical aspect alone, but have established principles of governance, risk management, privacy protection, compliance, incident response, and international cooperation, making the comparison between them and Saudi regulation of significant scientific and practical value, contributing to assessing the extent of alignment between the Saudi regulatory environment and international best practices, and revealing areas of strength as well as aspects that could be developed.

Herein lies the importance of this study, as it does not address cybersecurity as a purely technical subject, nor does it confine itself to studying data protection as a privacy right, but examines the integrative relationship between cybersecurity governance, data protection, and digital transactions from a comparative legal and regulatory perspective, aiming to set out the foundations underlying the legal protection of digital transactions, analyze Saudi regulation in light of international frameworks and standards, and ultimately build an integrated conception that strengthens digital trust, raises the level of compliance, and supports the sustainability of the digital economy.

On this basis, this study seeks to present a scholarly treatment combining theoretical grounding, statutory analysis, and international comparison, contributing to enriching Arabic legal scholarship on one of the most current and influential subjects for the future of digital transactions, and providing a framework that can be drawn upon in developing legislation and institutional policies relating to cybersecurity governance and data protection in the Kingdom of Saudi Arabia. Unlike previous studies which have addressed cybersecurity governance, data protection, and digital transactions as a single, interconnected system, whereas the majority of prior studies have addressed these subjects separately, some focusing on cybercrime, others on data protection, and others still on cybersecurity from a technical or economic perspective, while this research aims to integrate these dimensions within a single legal and regulatory framework founded on governance, risk management, and compliance. The proposed framework may support the work of regulatory and oversight bodies, boards of directors, compliance and risk-management departments, financial-technology service providers, and digital-service providers by offering an applied legal framework that helps strengthen compliance, raise the level of institutional maturity in the field of cybersecurity, and reduce the statutory and operational risks associated with digital transactions. While other Arabic legal studies of cybersecurity tend to analyze the matter mainly from the perspective of technology or criminal law, this study focuses on the institutional perspective of cybersecurity governance, which refers to governance, risk management, compliance, monitoring, and accountability in the process of digital transactions.

The research problem accordingly consists in the existence of a scholarly and practical need to build an integrated legal conception that defines the foundations underlying cybersecurity governance in digital transactions, determines the adequacy of Saudi regulation in achieving legal and regulatory protection, measures the degree of its alignment with international frameworks and standards, and arrives at a governance framework contributing to strengthening digital trust, protecting the digital economy, and sustaining electronic transactions.

On this basis, the research problem may be formulated in the following central question:

"To what extent do Saudi regulations achieve an integrated framework for cybersecurity governance and data protection in digital transactions, and to what extent is this framework consistent with international frameworks and standards to ensure the enhancement of digital trust, the management of cyber risk, and the protection of the legal rights of the parties to a transaction?"

To address this research problem, the study is guided by the following research questions and objectives.

1.1 Research Questions

In light of the research problem, this study seeks to answer the foregoing central question, from which the following sub-questions branch:

1. What is meant by cybersecurity governance, what is its legal nature, and how is it distinguished from information security and data protection?
2. What is the legal framework governing cybersecurity governance and data protection in digital transactions in the Kingdom of Saudi Arabia?
3. What role do institutional governance, risk management, compliance mechanisms, and statutory controls play in protecting digital transactions and ensuring effective cybersecurity governance?

4. To what extent is Saudi regulation consistent with international frameworks and standards, foremost among them NIST, ISO/IEC 27001, ISO/IEC 27701, and the European Union General Data Protection Regulation (GDPR)?
5. What deficiencies or challenges face the practical application of cybersecurity governance in digital transactions?
6. What legal and regulatory framework may be proposed to strengthen cybersecurity governance and data protection in the Kingdom of Saudi Arabia, consistent with international best practices?

1.2 Research Objectives

This research seeks to achieve a set of objectives consistent with the study's central problem and responsive to the rapid developments in the field of digital transactions and cybersecurity, as follows:

1. To establish the conceptual framework of cybersecurity governance and set out its legal nature and its relationship to information security, data protection, and digital transactions, while determining the points of agreement and divergence between these concepts, to remove the overlap surrounding them in legal and technical writing.
2. To analyze the Saudi legal and regulatory framework governing cybersecurity governance, data protection, and the legal liabilities arising from non-compliance.
3. To examine the role of institutional governance, risk management, compliance, and data-protection controls in strengthening cybersecurity and ensuring secure digital transactions.
4. To assess the extent of Saudi regulation's alignment with international frameworks and standards, foremost among them the NIST CSF 2.0, ISO/IEC 27001 and ISO/IEC 27701, the European Union General Data Protection Regulation (GDPR), and other relevant international references.
5. To propose an integrated legal and governance framework contributing to the development of the Saudi regulatory environment, and enhancing alignment with international best practices and standards, to support digital trust, raise the level of compliance, and achieve effective protection of digital transactions.

2. Literature Review

The subject of cybersecurity and data protection has received growing attention in legal and regulatory literature in recent years, coinciding with the expanding scope of digital transformation and the growing reliance on electronic transactions, financial technology, and digital services (WEF, 2024; OECD, 2022). This attention, however, has for the most part addressed scattered aspects of the subject: some studies have treated cybersecurity from a technical or security perspective, while others have focused on cybercrime, personal data protection, or the digital economy, without combining cybersecurity governance, data protection, and digital transactions within a comparative legal and regulatory framework (ITU, 2024).

2.1 Cybersecurity Governance

A growing body of legal and regulatory scholarship has addressed the concept of cybersecurity, its regulatory dimensions, and its role in protecting institutions and states from digital risks, most notably the study by Rashid Muhammad Al-Marri entitled "Cybersecurity and the Protection of Electronic Systems," which aimed to set out the concept of cybersecurity and analyze its role in protecting electronic systems, while addressing the legal, social, and security dimensions of cybercrime. It concluded that cybersecurity has become part of national security, and that protecting electronic systems requires developing legislation, raising awareness, strengthening international cooperation, and establishing specialized regulatory frameworks (Al-Marri, 2024).

Beyond doctrinal legal research, contemporary regulatory frameworks increasingly recognize that cybersecurity is a matter of governance, rather than just technology and criminal law. International standards and

Saudi regulations stress the importance of cybersecurity through accountability, risk management, regulatory compliance, and strategic oversight. Frameworks including the ISO/IEC 27001 standard, the NIST CSF 2.0, the National Cybersecurity Authority Essential Cybersecurity Controls (ECC), and the Saudi Arabian Monetary Agency (SAMA) Cyber Security Framework represent an example of this transformation from a security-driven approach into a governance-based model to support secure transactions (ISO, 2022; NIST, 2024; National Cybersecurity Authority, 2018; SAMA, 2023).

This study is among the important works establishing the concept of cybersecurity; it focused, however, primarily on the criminal and social protection of electronic systems, and did not address cybersecurity governance within the environment of digital transactions, nor did it link cybersecurity to data protection or modern regulatory frameworks (Al-Marri, 2024). The study by Said Ougane entitled "Cybersecurity and the Stakes of Digital Transformation" likewise addressed the impact of digital transformation in reshaping the concept of national security, analyzing the Moroccan strategy in the field of cybersecurity, with a comparison to certain international efforts, and concluded with the necessity of developing national legislation and strengthening international cooperation in confronting cyber risks (Oughane, 2023). In the same way, Al-Shammari and Ismail (2020) looked at cybersecurity as a new pillar in the national strategy of Iraq, emphasizing the increasing realization of cybersecurity as an issue of national security in the region.

The importance of this study is evident in its analysis of the relationship between cybersecurity and digital transformation; it tended, however, to study cybersecurity from the standpoint of national security and general strategy, and did not address the legal regulation of digital transactions, data protection, or institutional governance.

Collectively, these research studies show the increasing recognition of cybersecurity as an important legal and regulatory issue in the wake of digitalization. However, they tend to analyze cybersecurity from either the perspective of national security, legislative reforms, or cybercrime prevention without touching upon cybersecurity governance as an overarching concept covering issues such as accountability, data protection, compliance, and digital transactions. This limitation demonstrates the need for a more complete legal and governance-based analysis, which is provided by the present study.

2.2 Data Protection and Digital Privacy

This stream of literature examines the protection of personal data as one of individuals' fundamental rights, and is concerned with analyzing privacy legislation, particularly the European Union General Data Protection Regulation (GDPR), and comparative studies relating to data processing and cross-border transfer (European Parliament & Council, 2016; ISO, 2019).

Recent regulatory advancements have further consolidated the link between privacy and governance within organizations. The international regulations, including GDPR and ISO/IEC 27701, focus on accountability, transparency, lawful processing, and privacy management as the key principles of data governance. Likewise, Saudi Arabia has provided a legal basis for the protection of personal data through the PDPL and the Executive Regulations, forming the comprehensive legal framework for data gathering, processing, storing, and disclosing (European Parliament & Council, 2016; ISO, 2019; SDAIA, 2023).

Despite the considerable importance of these studies in establishing the legal principles relating to privacy, most of them addressed data protection as an independent subject, without linking it to cybersecurity governance, risk management, or the regulatory environment of digital transactions; most of them likewise did not address the Saudi experience following the issuance of the Personal Data Protection Law and its subsequent implementing regulations (SDAIA, 2023).

2.3 Cybercrime and Legal Liability

Another stream of legal scholarship examines cybercrime, its elements, its forms, the penalties prescribed for it, and the civil and criminal liability arising from it, focusing on crimes of intrusion, data theft, electronic fraud, phishing, and identity impersonation (Khalil, 2008; Hegazy, 2020).

The Saudi Anti-Cyber Crime Law is also responsible for establishing the legal grounds for the criminalization of unauthorized access, data interference, electronic fraud, and other forms of cybercrime, thus improving the legal security of digital systems and electronic transactions. However, the key focus of this legal research has been on criminal punishment and post-incident responsibility, not on the proactive approaches of cyber risk governance intended to prevent these risks (Anti-Cyber Crime Law, 2007).

These studies contributed to establishing the criminal foundation for cybercrime; they proceeded, however, from the notion of a crime occurring after an attack has taken place, whereas cyber governance is founded on a different philosophy, one of prevention, risk management, and institutional compliance before harm occurs, an aspect that has not received sufficient attention in most prior studies (Khalil, 2008; Hegazy, 2020).

2.4 Digital Economy and Financial Technology

The legal literature and the regulatory frameworks concerning the influence of digitalization on the digital economy, FinTech, e-commerce, and online banking services have recently focused on the critical importance of cybersecurity to ensure digital trust, safeguard financial transactions and the stability of digital markets (OECD, 2022; WEF, 2024; SAMA, 2023; Al-Baghdadi, 2021).

Moreover, international policy reports also acknowledge the importance of cybersecurity as one of the key factors that enable sustainable digital economic development instead of being viewed only as a technical tool. The governance of cybersecurity helps foster innovation, build consumer trust, protect the financial system, and facilitate cross-border digital transactions through confidentiality, integrity, and availability of digital information (OECD, 2022; ITU, 2024).

Some of these studies have pointed to the importance of cybersecurity in supporting the digital economy; they have, however, generally treated it as one of the requirements of technical infrastructure, without addressing it as a legal and regulatory framework founded on institutional governance, risk management, data protection, and compliance, which constitutes the core of the present study (OECD, 2022; WEF, 2024).

Table 1. Summary of Previous Literature

Theme	Representative Literature	Primary Focus	Research Gap
Cybersecurity Governance	Al-Marri (2024); Oughane (2023); NIST (2024); ISO/IEC 27001 (2022)	Governance, national cybersecurity strategies, institutional protection	Limited integration with digital transaction governance and Saudi regulatory frameworks
Data Protection and Privacy	GDPR (2016); PDPL (2023); ISO/IEC 27001 (2019)	Privacy rights, personal data processing, compliance	Limited linkage with cybersecurity governance and institutional risk management
Cybercrime and Legal Liability	Khalil (2008); Hegazy (2020); Anti-Cyber Crime Law	Criminal liability and cyber offences	Reactive legal approach with limited emphasis on preventive governance
Digital Economy and FinTech	SAMA (2023); OECD (2022); WEF (2024)	Digital trust, financial technology and electronic services	Cybersecurity primarily viewed as technical infrastructure rather than governance

2.5 Synthesis of Prior Studies and Research Gap

The above review shows that the current body of knowledge is successful in contributing to the understanding of issues related to cybersecurity, data protection, cybercrime, and the digital economy from the perspective of different legal frameworks and regulations. Despite the importance of conceptual and regulatory aspects raised in these studies, each of these dimensions is analyzed separately, leading to limited integration between cybersecurity governance, data protection, organizational compliance, and digital transactions.

Studies combining cybersecurity governance, data protection, and digital transactions within a comparative legal and regulatory framework, particularly in light of Saudi regulation together with international frameworks and standards, remain limited, particularly in light of the Saudi regulatory regime and its convergence with current international standards of governance. Therefore, the present research addresses this gap by conducting a combined legal and governance analysis of cybersecurity and data protection in digital transactions based primarily on the Saudi regulatory system while comparing it comprehensively with prominent international regulatory systems and standards.

3. Methodology

3.1 Research Design

This study uses a qualitative doctrinal legal research design to study the governance of cybersecurity and the protection of data in digital transactions in the Kingdom of Saudi Arabia. This is a doctrinal legal study, as it aims to understand and explain legal rules, statutory provisions, regulatory instruments and internationally recognised standards, rather than to produce empirical evidence gained from surveys, interviews or experiments. The research aims to identify the legal principles of cybersecurity governance, data protection, institutional compliance and digital transactions and assess their consistency in the Saudi regulatory context.

The study also includes qualitative legal analysis augmented by comparative legal reasoning to evaluate Saudi regulation in relation to internationally recognized cybersecurity and privacy frameworks, in order to determine the consistency of Saudi regulation with those frameworks. The design allows for a systematic study of the legal framework of digital transactions and the identification of strengths, weaknesses, and gaps in the regulation that need to be filled with new legislation.

3.2 Research Method

This study uses the doctrinal legal research method as it is a method that is systematic in identifying, interpreting, and critically analysing legal materials relevant to cybersecurity governance and data protection. This study analyzes legal requirements of a statutory nature, executive regulations, regulatory frameworks, official guidelines, and internationally recognized cybersecurity standards in order to assess the legal responsibilities of digital transactions (NIST, 2024; ISO, 2022).

A comparative legal approach is also used to evaluate and compare the Saudi legal system to the best international legal and regulatory standards. The comparison does not examine the legal systems themselves, but rather key principles of cybersecurity governance such as institutional accountability, managing cyber risk, regulatory compliance, protection of personal data, incident response, business continuity and legal liability. The Saudi legal framework is compared to the following international frameworks: NIST Cybersecurity Framework (NIST CSF 2.0), ISO/IEC 27001:2022, ISO/IEC 27701:2019, General Data Protection Regulation (GDPR), and the Budapest Convention on Cybercrime (NIST, 2024; ISO, 2022; ISO, 2019; European Parliament & Council, 2016).

The legal materials are analyzed qualitatively using doctrinal and thematic analysis, which helps articulate the legal and regulatory principles that are repeated, the convergence of laws, and the gaps in the existing regulatory framework that impact cybersecurity governance and the security of digital transactions.

3.3 Research Scope

The study focuses on the legal and regulatory aspects of cybersecurity governance and data protection in digital transactions, with a specific emphasis on the Saudi legal system and on existing international legal frameworks. The

research is limited to legal and regulatory review and does not attempt to make any judgment on the technical efficiency of cybersecurity techniques through empirical tests.

The analysis is not limited to cybersecurity technical issues such as software engineering, network architecture, encryption algorithms, or system design, unless a technical concept is referenced to explain its legal and regulatory applications. Similarly, a discussion on cybercrime is limited to its intersection with legal liability for the lack of cybersecurity governance and data protection and not treated as a standalone body of criminal law.

The practical analysis is carried out in areas where Cybersecurity governance directly has a regulatory impact, like financial technology (FinTech), electronic commerce, digital government services, electronic banking, digital payment systems and digital platforms.

3.4 Sources of Legal Materials

The study has used primary and secondary legal sources.

The legal materials used are mainly Saudi legislation and regulatory instruments directly related to cybersecurity and digital transactions, such as the Personal Data Protection Law (PDPL), the Electronic Transactions Law, the E-Commerce Law, the Anti-Cyber Crime Law, the Executive Regulations of the Personal Data Protection Law, the Saudi Central Bank (SAMA) Cybersecurity Framework, and the Capital Market Authority (CMA) Cybersecurity Guidelines (Saudi Data and Artificial Intelligence Authority, 2023; SAMA, 2023; National Cybersecurity Authority, 2018).

The comparative analysis is also based on legal and regulatory frameworks widely used internationally, such as the NIST CSF 2.0, ISO/IEC 27001:2022, ISO/IEC 27701:2019, the General Data Protection Regulation (GDPR) from the European Union, and the Convention on Cybercrime (Budapest Convention) of the Council of Europe (NIST, 2024; ISO, 2022; ISO, 2019).

Secondary legal materials are Arabic or international scholarly books, peer-reviewed journal articles, official reports, policy documents, and publications by international bodies such as the International Telecommunication Union (ITU), the Organisation for Economic Co-operation and Development (OECD), and the World Economic Forum (WEF).

Table 2. Legal and Regulatory Sources Examined in the Study

Category	Sources Examined
Saudi Legislation	Personal Data Protection Law (PDPL), Electronic Transactions Law, E-Commerce Law, Anti-Cyber Crime Law
Saudi Regulatory Frameworks	Essential Cybersecurity Controls (ECC), SAMA Cyber Security Framework, CMA Cybersecurity Guidelines
International Standards	NIST CSF 2.0, ISO/IEC 27001:2022, ISO/IEC 27701:2019
International Legal Instruments	General Data Protection Regulation (GDPR), Budapest Convention on Cybercrime
Secondary Sources	Peer-reviewed journal articles, legal books, official reports, policy documents, and publications from ITU, OECD, and WEF

3.5 Analytical Approach

The legal documents presented in Table 2 have been analyzed using a thematic doctrinal approach that considered cybersecurity governance from four interdependent perspectives.

The first dimension focuses on the concept and legal aspects of cybersecurity governance and data protection in Saudi Arabia. The second assesses the governance of institutions, regulatory compliance, and mechanisms for managing cyber risk in the context of digital transactions. The third examines civil, regulatory, and criminal liability

in the event of a failure in cybersecurity governance and data protection. Lastly, the fourth section takes the Saudi regulatory environment and practices and compares them to internationally accepted legal and regulatory best practices to find areas of convergence, divergence, and possible legislative development. The methodological components discussed in this study are summarized in Table 3.

Table 3. Methodological Framework of the Study

Component	Description
Research Design	Qualitative doctrinal legal research
Research Method	Doctrinal and comparative legal analysis
Primary Sources	Saudi laws, regulations and regulatory frameworks
Secondary Sources	Books, peer-reviewed literature and official reports
Comparative Standards	NIST CSF 2.0, ISO/IEC 27001, ISO/IEC 27701, GDPR, Budapest Convention
Analytical Technique	Thematic legal analysis
Research Focus	Cybersecurity governance and data protection

3.6 Limitations of the Study.

This study has a few limitations.

First, it is limited to the legal and regulatory aspects of cybersecurity governance and does not assess the effectiveness of cybersecurity controls empirically or by engineering analysis. Second, this comparative assessment does not make a complete comparison of the national legal systems, but only selected international legal frameworks and regulatory standards that have had a significant impact on the current governance of cybersecurity and data protection. Third, the study is based on the Saudi legislative and regulatory framework in addition to the relevant international standards as they stand at the time of writing. The legal framework and governance mechanisms studied in this research may need to be reviewed in the future, as the cybersecurity landscape keeps changing in tandem with digital technologies.

Based on the foregoing methodological approach, the following sections provide a basis for understanding the legal and regulatory frameworks of cybersecurity and data protection in Saudi Arabia.

4. Legal and Regulatory Framework of Cybersecurity Governance

Digital transactions have come to constitute the principal framework for conducting economic, financial, and administrative activities amid digital transformation, making data protection and the securing of digital systems a fundamental condition for the stability and continuity of such transactions (OECD, 2022; UNCTAD, 2024). Cybersecurity is no longer confined to being a technical means of protecting digital infrastructure, but has developed into an integrated governance framework founded on risk management, the determination of responsibilities, the strengthening of compliance, and the protection of digital rights, thereby ensuring the safety of the digital environment and strengthening trust in it.

The study of cybersecurity governance accordingly requires beginning with the identification of the basic concepts underlying this field, followed by an account of the statutory basis adopted by the Kingdom of Saudi Arabia for its regulation, as a prelude to examining governance mechanisms, risk management, and legal liability in the subsequent sections.

Proceeding from this, this section addresses the concept of digital transactions and their legal characteristics, then sets out the concept of cybersecurity governance and its relationship to information security and data protection, before surveying the Saudi statutory framework governing this field in light of national laws and international frameworks and standards.

4.1 Digital Transactions: Concept and Legal Characteristics

Digital transactions are an inherent element of today's digital transformation, which is transforming numerous paper-based transaction processes such as those related to contracting, money, and administration, into electronic channels of communication. This transformation has shifted the transaction from its traditional form into a digital environment characterized by speed, decentralization, and reliance on data as the principal axis for concluding and performing legal acts.

The concept of digital transactions is not confined to the mere use of electronic means in exchanging information, but extends to encompass all legal, financial, and administrative acts that arise, are performed, are evidenced, or are retained using digital media, including electronic contracts, digital payment operations, electronic bank transfers, financial-technology services, electronic signatures, smart contracts, digital government services, and other applications that have come to form the basic infrastructure of the digital economy. The increasing number of digital transactions has benefited from regulation in terms of emphasis on legal recognition of electronic communication, digital identification, interoperability, and security of electronic services, thus increasing trust in digital transactions (OECD, 2022).

From a legal standpoint, digital transactions are distinguished by three principal elements: the first is the digital data that constitutes the subject matter of legal protection; the second is the electronic medium through which data is exchanged or the transaction is performed; and the third is the digital trust on which the lawfulness of the dealing and its capacity to be relied upon and proven rest. The integrity, confidentiality, and availability of data have accordingly become essential elements in the validity of the transaction and the stability of its legal effects, which explains the close connection between the regulation of digital transactions and the rules of cybersecurity and data protection (ISO, 2022; NIST, 2024).

The Saudi legislator has recognized this particular nature of digital transactions, and has accordingly worked to build an integrated statutory framework regulating their various aspects, beginning with the legal recognition of electronic dealings, continuing through the regulation of e-commerce, and extending to the protection of personal data and the criminalization of attacks on information systems, together with the issuance of the Essential Cybersecurity Controls (Electronic Transactions Law, 2007; E-Commerce Law, 2019; PDPL, 2023; NCA, 2018). This orientation reflects a shift in legislative policy from regulating the electronic medium itself to regulating the digital environment in all its elements.

The regulatory guides issued by the National Cybersecurity Authority likewise confirm that e-commerce and digital transactions depend on the protection of systems, data, customer accounts, and payment operations, and that preserving digital trust requires the application of integrated controls including strong authentication, network protection, encryption, data management, continuous training, and business continuity (National Cybersecurity Authority, 2022).

Table 4. Essential Legal Characteristics of Digital Transactions

Characteristic	Legal Significance	Regulatory Importance
Electronic form	Legal recognition of transactions	Electronic Transactions Law
Digital data	Subject of legal protection	PDPL
Authentication	Identity verification	ECC, SAMA
Integrity	Prevents alteration	ISO/IEC 27001
Confidentiality	Protects personal information	PDPL, GDPR
Availability	Service continuity	NIST CSF

These characteristics indicate that not only the legality of electronic transactions, but also the existence of governance processes to ensure confidentiality, integrity, availability, accountability, and regulatory compliance is

required to facilitate digital transactions. Accordingly, cybersecurity governance has become an essential legal necessity to ensure the functioning of the digital economy.

4.2 Cybersecurity Governance, Information Security, and Data Protection

The growing reliance on digital transactions has driven the evolution of cybersecurity from a set of technical measures aimed at protecting networks and systems into an integrated institutional system grounded in governance, risk management, compliance, oversight, and business continuity. An institution's success in protecting its digital assets is accordingly no longer measured merely by its possession of advanced technical means, but by its capacity to build a governance framework that defines responsibilities, allocates authority, and ensures that cybersecurity-related decisions are made within the senior management system (NIST, 2024; ISO, 2022).

Cybersecurity governance refers to organizational policies, roles, and controls meant to manage cyber risks, align security activities with regulations, safeguard the organization’s information assets, and assure continuity of services. Therefore, the role of cybersecurity has changed from an IT-related technical process to a governance issue requiring the involvement of senior management, compliance, auditing, and risk management departments. (ISO, 2022; NCA, 2018).

This trend is clearly reflected in Saudi regulatory guides: the Cybersecurity Guidelines for Capital Market Institutions make the board of directors the party primarily responsible for cybersecurity, and require the establishment of an independent cybersecurity department and a dedicated committee, the determination of responsibilities, the adoption of policies, risk management, and continuous auditing, confirming that governance has become the foundation on which the institution's cybersecurity system rests (Capital Market Authority, 2023).

Defining the concept of governance further requires distinguishing between cybersecurity and information security, as the two terms are frequently used synonymously despite differing in scope. Information security is the broader concept, aiming to protect information in all its forms whether paper-based, digital, or oral, by preserving its confidentiality, integrity, and availability. Cybersecurity, by contrast, relates to protecting the digital environment itself, including the networks, systems, applications, devices, and digital services it comprises, from attacks, breaches, and unlawful exploitation. Cybersecurity accordingly represents one of the principal components of information security, rather than a substitute for it (ISO/IEC 27001, 2022).

Cybersecurity is closely connected to data protection, as data represents the most valuable asset in the digital environment, whether personal, financial, commercial, or operational data. Data protection has accordingly become one of the principal objectives of cybersecurity governance, not only through preventing unauthorized access to it, but also by ensuring its integrity, the possibility of its recovery, the regulation of its circulation, and the disclosure of any incidents affecting it in accordance with statutory controls (ISO/IEC 27701, 2019; PDPL, 2023).

In this context, recent international frameworks confirm that effective cybersecurity governance is not achieved merely by applying technical solutions, but requires an institutional framework based on continuous risk assessment, the determination of the institution's risk appetite, the establishment of clear policies, the allocation of responsibilities, performance measurement, and continuous development. Governance has accordingly become a common element in most international frameworks, foremost among them the NIST CSF 2.0 and ISO/IEC 27001, which view cybersecurity as a continuous process of risk management and the achievement of institutional compliance (NIST, 2024; ISO, 2022). In another research perspective, Al-Tayyar (2020) explored cybersecurity from an Islamic legal perspective by proving that the safeguarding of digital data and operations is fully consistent with the wider goals of Sharia in protecting life, property, and public interest. Likewise, Jaballah (2022) carried out an important jurisprudential study, where he compared various methods of protecting cyberspace security with modern systems, adding new dimensions to the conceptualization of cybersecurity governance in the Arab jurisprudence tradition.

Table 5. Comparison between Information Security, Cybersecurity, and Data Protection

Aspect	Information Security	Cybersecurity	Data Protection
--------	----------------------	---------------	-----------------

Main objective	Protect information	Protect digital systems	Protect personal data
Scope	Physical & digital	Digital environment	Personal information
Core principles	CIA Triad	Risk management	Privacy, accountability
Primary standards	ISO/IEC 27001	NIST CSF, ECC	GDPR, ISO/IEC 27701, PDPL
Governance focus	Information assets	Cyber risk	Privacy compliance

Therefore, it can be concluded that cybersecurity governance, information security and data protection are complementary components of an overall regulatory framework for digital transactions. Information security is the goal of protecting information; cybersecurity is the set of practices that protect the digital environment in which information is stored; and information governance is institutional accountability, risk management, regulatory compliance and business continuity. As a result, cybersecurity governance has become a legal and regulatory duty to ensure digital trust and serve as a basis for the Saudi statutory framework outlined in the next subsection.

Figure 1 below illustrates a conceptual linkage between digital transactions, cybersecurity governance, information security and data protection, showing how governance combines legal, technical and organizational elements to create digital trust.

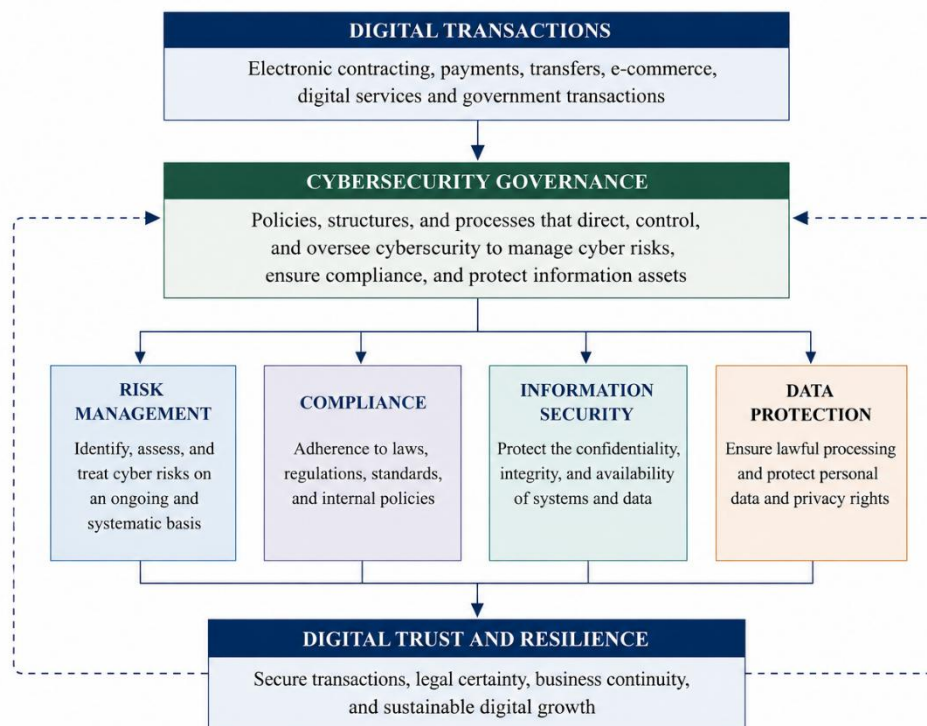


Figure 1. Conceptual Relationship between Digital Transactions, Cybersecurity Governance, and Data Protection

Source: Developed by the author based on NIST (2024), ISO/IEC 27001:2022, ISO/IEC 27701:2019, and PDPL (2023).

4.3 Saudi Legal and Regulatory Framework for Cybersecurity Governance

The Kingdom of Saudi Arabia has witnessed, in recent years, rapid legislative and regulatory development in the field of cybersecurity and data protection, coinciding with the state's adoption of the digital-transformation project

as one of the principal pillars of Saudi Vision 2030. This development has not been confined to issuing scattered laws addressing specific aspects of the digital environment, but has moved toward building an integrated regulatory system founded on the distribution of competencies among regulatory bodies, and linking cybersecurity to institutional governance, risk management, data protection, and business continuity (Vision 2030; NCA, 2018).

This statutory framework rests on a set of laws, regulations, and controls that integrate with one another to achieve a single objective: providing a secure digital environment that ensures data protection, strengthens trust in digital transactions, and preserves the stability of economic and financial sectors. Foremost in this system is the Personal Data Protection Law, which established a legal framework regulating the collection, processing, and disclosure of data and the protection of data subjects' rights, consistent with recent international trends in privacy protection (PDPL, 2023). The Electronic Transactions Law has likewise contributed to conferring legal probative value on electronic means, regulating the electronic signature, and establishing trust in legal acts concluded through digital media (Electronic Transactions Law, 2007). The E-Commerce Law has regulated the relationship between service providers and consumers and established statutory obligations aimed at strengthening trust and transparency in the digital environment (E-Commerce Law, 2019).

Alongside these laws, the National Cybersecurity Authority has played a pivotal role in building the national cybersecurity framework through the issuance of the Essential Cybersecurity Controls and sector-specific guidelines, which have moved regulation from mere technical protection to building an integrated system of governance, risk management, and compliance. The Cybersecurity Guidelines for E-Commerce Providers have clarified that protecting the digital environment rests on seven principal pillars, comprising strong authentication, systems protection, minimizing the impact of data breaches, account protection, network security, continuous awareness, and the protection of internal infrastructure, reflecting the comprehensiveness of Saudi regulation in this field (NCA, 2018).

Sectoral regulatory bodies have likewise given particular attention to cybersecurity governance, as the Saudi Central Bank and the Capital Market Authority have issued specialized regulatory frameworks requiring financial institutions to apply advanced controls in managing cyber risk, incident management, data protection, business continuity, and vendor management, consistent with the nature of the risks associated with the financial sector. Notable in this context is the Cybersecurity Guidelines for Capital Market Institutions, which makes governance, risk management, auditing, incident management, and third-party security fundamental elements in building the institution's security system (SAMA, 2023; CMA, 2023).

Table 6. Saudi Cybersecurity and Data Protection Regulatory Framework

Regulation	Institution	Primary Purpose
Personal Data Protection Law	SDAIA	Privacy and personal data protection
Electronic Transactions Law	Government	Legal validity of electronic transactions
E-Commerce Law	Ministry of Commerce	Consumer protection
Anti-Cyber Crime Law	Government	Criminal liability
Essential Cybersecurity Controls	NCA	National cybersecurity governance
SAMA Cyber Security Framework	SAMA	Financial sector governance
CMA Cybersecurity Guidelines	CMA	Capital market governance

In the Saudi governance system, an integrated legislative strategy is followed where the cybersecurity governance strategy involves the implementation of legislation, regulations, national-level controls, and industry regulations but not as one single comprehensive law. The Essential Cybersecurity Controls set by the National Cybersecurity Authority provide the national framework, whereas the sectoral regulators, including SAMA and the Capital Market Authority, add to that by providing sector-specific requirements. The integrated framework offers

regulatory flexibility, is consistent with international governance concepts, and forms the foundation of law for the governance, risk management, and compliance approaches discussed in the next section.

5. Governance, Compliance, and Cyber Risk Management in Digital Transactions

The success of a cybersecurity system is no longer measured merely by the existence of advanced technical means or electronic protection systems, but is now measured by the institution's capacity to build an integrated governance system that embeds cybersecurity within decision-making, risk management, regulatory compliance, and internal oversight. Digital transformation and the accompanying expansion in digital transactions have created an environment characterized by multiple sources of risk, making proactive risk management and compliance with statutory requirements among the most important elements of data protection and business continuity (NIST, 2024; ISO, 2022; OECD, 2022).

Proceeding from this, modern regulation no longer views cybersecurity as the sole responsibility of the information-technology department, but regards it as an institutional responsibility beginning with the board of directors and extending to all managerial levels, through the adoption of clear policies, the determination of responsibilities, risk management, the strengthening of compliance, and the application of operational controls that ensure the protection of data and digital transactions (NCA, 2018; CMA, 2023).

5.1 5.1 Institutional Governance of Cybersecurity and the Responsibility of Senior Management

Cybersecurity, in modern regulatory thought, is no longer an operational matter confined to protecting systems and networks, but has become one of the elements of institutional governance directly connected to the institution's strategic management (NIST, 2024; ISO, 2022). This shift rests on the recognition that cyber risks no longer threaten technical infrastructure alone, but have come to affect business continuity, institutional reputation, statutory obligations, and the financial rights of the parties to a transaction, requiring senior management's oversight of the management of these risks within the institutional governance framework.

For this reason, modern laws and regulatory frameworks have moved toward placing ultimate responsibility for cybersecurity on the board of directors, as the body competent to adopt the strategy, approve policies, determine the institution's risk appetite, monitor performance indicators, and ensure the allocation of the resources necessary to protect digital assets (CMA, 2023; SAMA, 2023). The board's role is no longer confined to approving periodic reports, but has become one of ensuring that cybersecurity is embedded within the governance, risk-management, and decision-making system.

Saudi regulation has clearly adopted this approach: the Cybersecurity Guidelines for Capital Market Institutions require the establishment of an independent cybersecurity department, the appointment of a dedicated director, and the establishment of a cybersecurity committee reporting to senior management, while determining the responsibilities of the board of directors in adopting the strategy and policies, overseeing risk management, monitoring performance indicators, and ensuring compliance with regulatory requirements (CMA, 2023; SAMA, 2023).

Institutional governance is not confined to the distribution of competencies, but extends to building an institutional culture that makes cybersecurity part of the day-to-day work system, through the adoption of written policies, the establishment of lines of accountability, and linking cybersecurity to compliance management, internal review, and risk management, to achieve integration between the legal, regulatory, and operational dimensions (Al-Samhan, 2020; ISO, 2022).

International frameworks, foremost among them the NIST CSF 2.0, confirm that the Govern function has become the foundation on which the other cybersecurity functions are built, reflecting the shift of governance from being a managerial element into a strategic requirement for risk management and achieving institutional compliance (NIST, 2024; ISO, 2022). This trend is observed to be substantially consistent with the approach adopted by Saudi regulation, reflecting an advanced level of alignment with international practices.

Effective institutional governance not only involves the creation of the organizational structures for cybersecurity but also involves role definition, the maintenance of cybersecurity independence, inclusion of cyber risk in strategic decisions, and continuous supervision by senior management. Institutional governance thus represents the starting point in building the cybersecurity system, while cyber risk management represents the executive tool that translates this governance into practical procedures, a matter addressed in the following subsection.

5.2 Cybersecurity Risk Management, Review, and Auditing

Cybersecurity risk management constitutes the practical pillar on which cybersecurity governance rests, representing the mechanism through which policies and strategies are translated into implementing procedures aimed at continuously identifying, analyzing, assessing, and treating risk. Risk management in the digital environment is no longer confined to addressing technical threats, but has become part of the enterprise risk-management system, given the direct impact of cyber risk on an institution's financial position, business continuity, statutory obligations, and the trust of those dealing with it (ISO 31000, 2018; NIST, 2024).

Risk management begins with an inventory of valuable digital assets, whether data, applications, operating systems, infrastructure, or digital services, followed by identifying potential sources of threat, analyzing their likelihood, and measuring their expected impact, before selecting the appropriate treatment measures, whether by reducing, transferring, avoiding, or accepting the risk within the limits approved by senior management (ISO, 2022). This process is characterized by its continuous nature, as cyber risks change at an accelerating pace, requiring periodic review rather than reliance on an initial assessment alone.

Saudi regulation has clearly adopted this approach, as the Cybersecurity Guidelines for Capital Market Institutions require the establishment of a documented methodology for cybersecurity risk management consistent with the institution's overall risk-management methodology, comprising the identification, analysis, response to, monitoring, and periodic review of risks, with priority given to high-impact risks, their documentation in a unified risk register, and the conduct of risk assessments when implementing new projects, introducing material changes to technical infrastructure, or contracting with external parties.

The risk-management process does not end merely with the establishment of treatment plans, but requires an effective oversight system that measures compliance with these plans, monitors any change in the level of risk, and assesses the efficiency of the controls applied. Herein lies the importance of cyber review and auditing as two means of verifying the effectiveness of the cybersecurity system, the institution's compliance with statutory requirements and regulatory controls, and the early detection of weaknesses that may lead to cyber incidents (CMA, 2023).

Within this framework, the internal-audit function is no longer confined to reviewing financial and administrative operations, but has extended to reviewing cybersecurity controls, measuring their efficiency, and verifying their implementation in accordance with approved policies, while submitting periodic reports to senior management containing observations, recommendations, and treatment plans. Penetration testing, vulnerability assessment, systems-configuration review, and event-log analysis have likewise become fundamental tools for assessing institutions' level of cyber maturity (NIST, 2024).

These trends are consistent with international frameworks, which make risk management and continuous review the basis for achieving cyber resilience, since it is not sufficient to prevent attacks absolutely; rather, the institution must be capable of detecting, responding to, and recovering from them with the least possible losses — requiring the integration of risk management with business-continuity plans and crisis management.

Effective cyber risk management requires the integration of risk assessment, continuous monitoring, auditing, and control improvement to enable effective decision-making, regulatory compliance, and strengthen operations.

5.3 Operational Controls for Data Protection in Digital Transactions

Operational controls represent the executive link in the cybersecurity governance system, through which policies and strategies are translated into practical procedures aimed at protecting digital data and systems during their

operation and use. If governance determines responsibilities and risk management measures the level of exposure to threats, operational controls are the means that prevent those risks from materializing or limit their effects when they occur, making them a principal criterion for measuring institutions' efficiency in protecting digital transactions (NCA, 2018; ISO, 2022).

These controls rest on a fundamental principle: that data protection is not achieved through a single measure, but through an integrated system comprising access-control management, encryption, digital-identity management, application protection, vulnerability management, incident monitoring, and business continuity, such that these procedures integrate to protect data throughout its lifecycle, from collection and processing to retention or destruction in accordance with statutory controls (ISO, 2022; ISO/IEC 27701, 2019).

Saudi laws and controls have given considerable attention to these aspects: the Cybersecurity Guidelines for Capital Market Institutions set out a wide range of operational controls, comprising access-identity and privilege management, infrastructure protection, information-asset management, incident management, event-log management, threat management, application protection, encryption, vulnerability management, business continuity, and third-party security, reflecting the comprehensiveness of the Saudi regulatory system in addressing the various stages of protecting data and digital transactions.

Table 7. Operational Cybersecurity Controls for Digital Transactions

Operational Control	Primary Objective	Relevant Framework
Identity and Access Management	Restrict unauthorized access	NIST CSF; ISO/IEC 27001; ECC
Multi-Factor Authentication	Strengthen user verification	NCA ECC; SAMA
Encryption	Protect data confidentiality	ISO/IEC 27001; PDPL
Vulnerability Management	Identify and remediate weaknesses	NIST CSF
Security Monitoring & Logging	Detect abnormal activities	ISO/IEC 27001
Incident Response	Minimize operational impact	NIST CSF
Backup & Disaster Recovery	Ensure business continuity	ISO/IEC 27001
Third-Party Security	Manage vendor risks	SAMA; CMA

An analysis of the relationship between institutional governance, cyber risk management, compliance, operational controls, and continuous monitoring in enhancing digital transaction security is presented in Figure 2 below.

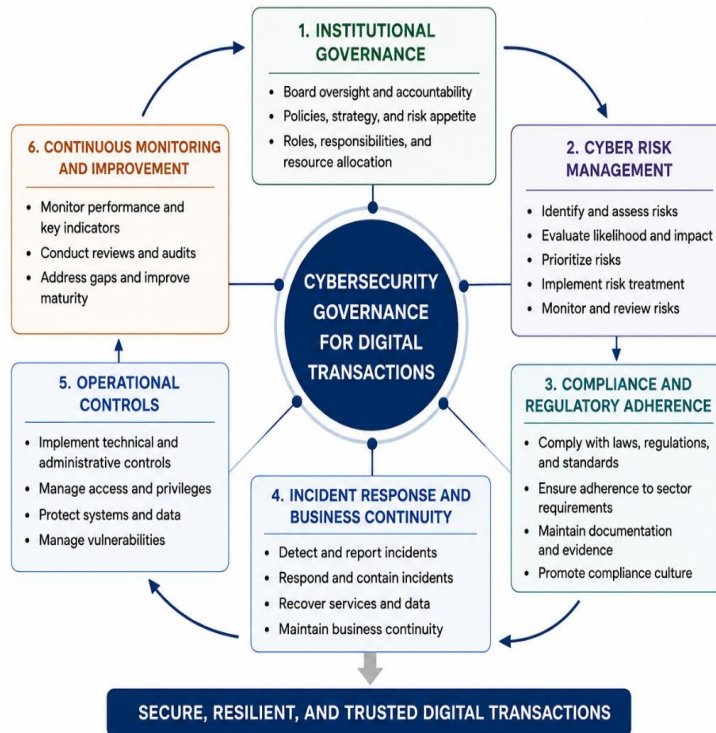


Figure 2. Integrated Cybersecurity Governance Framework for Digital Transactions

Source: Developed by the author based on NIST CSF 2.0, ISO/IEC 27001:2022, NCA Essential Cybersecurity Controls, SAMA Cyber Security Framework, and CMA Cybersecurity Guidelines.

Identity and privilege management is foremost among these controls, being based on restricting access to data to authorized persons, in accordance with the principle of least privilege, together with the use of strong verification means such as multi-factor authentication and periodic review of user accounts, reducing the risk of unlawful access or misuse of privileges.

Encryption likewise represents one of the most important legal and technical means of protecting data, as it prevents data from being exploited even in the event of unlawful access to it, whether during its transmission across networks or during its storage in databases or cloud environments. Backup management and business continuity also acquire particular importance, as they ensure the recovery of data and services in the event of failures or cyberattacks, particularly ransomware attacks, which have become among the most impactful threats to digital transactions.

Cyber-incident management, moreover, constitutes a fundamental element of operational controls, as the objective is no longer to prevent all incidents absolutely, but to ensure their rapid detection, containment, and reporting, the analysis of their causes, and the adoption of corrective measures preventing their recurrence. Saudi regulatory controls have accordingly required the existence of specialized incident-response teams, the documentation of incidents, and the reporting of material incidents to the competent authorities, while retaining the records necessary for investigation and review.

The importance of vendor and third-party management is likewise evident, given the reliance of many institutions on cloud-service providers or companies specialized in operating systems or processing data, which extends cyber risk beyond the boundaries of the institution itself. Assessing the risks associated with third parties, incorporating cybersecurity requirements into contracts, and monitoring vendor compliance have accordingly become an integral part of the protection system.

Operational controls determine the effectiveness of cybersecurity governance. The implementation of operational controls will be successful if it is continuously integrated with the governance framework and cyber risk management for secure, resilient, and compliant digital transactions.

6. Legal Liability and International Comparative Analysis

The system of cybersecurity governance is not complete merely with the establishment of regulatory controls or the application of technical measures, but requires a legal system that determines the liability arising from breach of protection requirements, prescribes the appropriate sanctions to ensure compliance, and guarantees redress for harm arising from attacks on data or digital systems (NIST, 2024; ISO/IEC 27001, 2022). Legal liability represents the tool through which governance rules move from the stage of regulation to the stage of enforceability, thereby strengthening trust in digital transactions and ensuring their stability.

Modern laws have moved toward adopting an integrated concept of liability, not confined to criminal penalties but extending to civil and regulatory liability, linked to governance requirements, risk management, and the disclosure of cyber incidents (OECD, 2022; UNCTAD, 2024). International frameworks and standards have likewise shown notable development in this field, through establishing unified rules for data protection and strengthening international cooperation in confronting cybercrime, highlighting the importance of comparing Saudi regulation with these international references.

This section accordingly addresses civil and regulatory liability for breach of cybersecurity, then criminal liability for cybercrimes affecting digital transactions, and finally the comparison with international frameworks and standards, leading to a proposed legal framework that strengthens cybersecurity governance and data protection.

6.1 Civil and Regulatory Liability for Breach of Cybersecurity and Data Protection

The impact of breaching cybersecurity requirements in the digital environment is no longer confined to the loss of data or the disruption of systems, but extends to harming individuals' rights, exposing institutions to regulatory accountability, and breaching their contractual and regulatory obligations (PDPL, 2023; GDPR, 2016). Modern legislation has accordingly moved toward expanding the scope of legal liability to encompass any entity that fails to take reasonable measures to protect data or manage cyber risk, regardless of whether a direct attack on systems has occurred.

Civil liability in this field rests on breach of the legal or contractual obligation to protect data, preserve its confidentiality, or ensure the integrity of digital systems. Where such breach results in harm to customers, other parties to a transaction, or third parties, the liability of the responsible entity is established provided the elements of liability, fault, harm, and causal connection are present. Compensation is not confined to material harm, but may extend to the moral and economic harm arising from loss of privacy, service disruption, or damage to commercial reputation (PDPL, 2023; OECD, 2022).

Regulatory liability, for its part, rests on the violation of laws, regulations, or controls issued by regulatory bodies, even where no actual harm is proven, as breach of the statutory requirements relating to data protection, risk management, or incident disclosure suffices to trigger the prescribed administrative and regulatory sanctions (NCA, 2018; CMA, 2023). This trend reflects the shift from addressing the consequences of a cyber incident to requiring institutions to take preventive measures forestalling its occurrence.

Saudi regulatory guides have confirmed this trend by requiring institutions to establish an integrated system for cyber-incident management, document incidents, report material incidents, and take corrective measures, making compliance with regulatory controls part of the institution's statutory liability (CMA, 2023; NCA, 2018).

The development of civil and regulatory liability in the digital environment reflects the shift of legislation from the concept of liability arising after harm occurs to the concept of preventive liability, which requires institutions to manage risk before it materializes, consistent with the philosophy of cybersecurity governance, which makes

prevention and compliance part of the legal obligation itself, rather than merely a means of fulfilling it (OECD, 2022; ISO, 2022).

6.2 Criminal Liability for Cybercrimes Affecting Digital Transactions

The rapid development of digital transactions has required modern legislation to reconsider traditional criminal-protection means, as attacks are no longer directed solely at money or physical instruments, but now target data, systems, networks, and digital infrastructure — elements that today form the foundation of economic, financial, and administrative activity. Most legislation has accordingly moved toward criminalizing acts affecting the security of the digital environment, regarding them as an attack on trust in digital transactions and their stability, rather than a mere attack on technical media.

Cybercrimes affecting digital transactions are diverse, including crimes of unlawful access to systems, the interception, copying, alteration, or destruction of data, electronic fraud, digital identity theft, phishing, ransomware, service disruption, and manipulation of payment and money-transfer systems, all of which share the common feature of targeting the integrity of the digital environment underlying electronic transactions, and directly affecting economic trust and legal security (Anti-Cyber Crime Law, 2007; UNODC, 2021).

The Saudi legislator has addressed these crimes through the Anti-Cyber Crime Law, which criminalizes forms of attack on systems, data, and networks, and prescribes varying penalties according to the nature of the act and its consequences, to achieve general and specific deterrence and preserve the security of electronic dealings (Anti-Cyber Crime Law, 2007). It is noted that the Law is not confined to protecting government systems, but extends its protection to all information systems, including commercial and financial systems and digital services, reflecting the comprehensiveness of criminal protection in the digital environment.

Criminal liability is not confined to the natural person who commits the criminal act, but may extend to legal persons where their gross negligence in complying with statutory duties is established to have led to, or facilitated, the commission of the crime, in accordance with the general rules of liability and the regulatory sanctions prescribed by special laws (Anti-Cyber Crime Law, 2007). Institutions have accordingly become required to take effective preventive measures, not only to avoid operational risk, but also to limit their exposure to legal accountability.

Among the most prominent characteristics of cybercrime is that it frequently transcends the geographic borders of the state, as the perpetrator of the crime may be in one country, the targeted data in another, and the resulting harm in a third, raising issues relating to judicial jurisdiction, applicable law, the enforcement of judgments, the collection of digital evidence, and international judicial cooperation (Budapest Convention, 2001; UNODC, 2021). Combating these crimes has accordingly come to depend substantially on cooperation among competent authorities, the exchange of information, and mutual legal assistance.

In this context, recent legal studies confirm that cybercrimes differ from traditional crimes in terms of the subject matter of the attack, the speed of their commission, the difficulty of their detection and proof, and their reliance on sophisticated technical means, requiring the development of investigative and evidentiary tools, the training of specialized personnel, and the strengthening of international cooperation in combating cybercrime (UNODC, 2021).

Criminal protection represents the final layer of cybersecurity governance because it is an activity that starts after an occurrence, but cybersecurity governance focuses on prevention through risk management, compliance, oversight, awareness, and auditing (NIST, 2024; ISO, 2022). The effectiveness of the legal protection of digital transactions is accordingly not achieved by stiffening penalties alone, but by integrating criminal liability with civil and regulatory liability, within a comprehensive preventive system that reduces the chances of a crime occurring rather than merely addressing its effects after it has occurred.

It thus becomes clear that criminal liability represents one of the fundamental pillars for protecting the digital environment; achieving comprehensive protection, however, remains linked to the extent to which national legislation aligns with modern international trends — requiring an examination of the relevant international frameworks and

standards, and an account of the extent to which Saudi regulation is consistent with them, a matter addressed in the following subsection.

6.3 Comparative Analysis of Saudi and International Cybersecurity Frameworks

Cybersecurity is no longer a purely internal regulatory matter confined to the borders of the state, but has become part of the global governance system for digital transactions, owing to the cross-border nature of data, digital services, e-commerce platforms, and financial technology. International organizations and specialized bodies have accordingly moved toward establishing unified frameworks and standards aimed at strengthening cybersecurity, managing risk, protecting data, and achieving a minimum degree of alignment among national systems, so as to support trust in the global digital economy (OECD, 2022; UNCTAD, 2024).

Most of these frameworks, despite differing in legal nature, converge on a set of fundamental principles, the most important being: treating cybersecurity as an institutional responsibility beginning with senior management, linking protection to risk management, adopting written policies, determining responsibilities, protecting data throughout its lifecycle, rapid incident response, and the continuous improvement of security controls (NIST, 2024; ISO, 2022). These principles are no longer confined to technical standards, but represent requirements of institutional governance and management.

Prominent in this field is the Cybersecurity Framework issued by the (US) National Institute of Standards and Technology (NIST CSF), which is founded on a risk-management-based approach and links governance, risk identification, protection, detection, response, and recovery, providing a flexible framework that can be adapted to the nature of each institution. ISO/IEC 27001 likewise represents the foremost international reference for establishing and operating information security management systems, while ISO/IEC 27701 has expanded to regulate privacy-information management and the protection of personal data, reflecting the close connection between cybersecurity and data protection.

The European Union General Data Protection Regulation (GDPR), for its part, has established an advanced model for regulating the protection of personal data, founded on the principle of accountability, risk management, incident disclosure, and the protection of data subjects' rights, making it an influential reference in much national legislation, even beyond the European Union (GDPR, 2016).

Comparing these frameworks with the Saudi system reveals a substantial degree of alignment in general principles, particularly linking cybersecurity to governance, risk management, data protection, business continuity, and the determination of senior management's responsibilities. The controls issued by the National Cybersecurity Authority and the regulatory frameworks of the Saudi Central Bank and the Capital Market Authority likewise reflect the Kingdom's adoption of an institutional approach close to international trends, while considering the particularities of the national regulatory environment (NCA, 2018; SAMA, 2023; CMA, 2023).

Table 8. Comparative Analysis of Saudi Cybersecurity Governance and International Frameworks

Governance Dimension	Saudi Framework	NIST CSF 2.0	ISO/IEC 27001	GDPR
Governance	NCA ECC, CMA, SAMA	Govern Function	ISMS Governance	Accountability Principle
Risk Management	Mandatory sectoral risk assessment	Risk-based	Risk-based	Risk-based processing
Data Protection	PDPL	Covered indirectly	ISO/IEC 27701 integration	Core objective
Incident Response	Mandatory reporting	Respond & Recover	Incident Management	72-hour notification

Senior Management	Board responsibility	Governance leadership	Top management commitment	Data controller accountability
Compliance	Sector regulators	Voluntary framework	Certification standard	Legal obligation

The comparison indicates a high level of convergence between the Saudi cybersecurity governance framework and the international standard. Although implementation mechanisms differ, each framework highlights governance, risk management, accountability, incident handling, and continuous improvement as core elements of digital trust.

Nevertheless, the continuous development of digital technologies requires the continued updating of regulatory controls, the strengthening of integration among regulatory bodies, and the unification of certain concepts and procedures relating to incident reporting, third-party risk management, and data governance, to ensure the maintenance of the level of alignment with rapid international developments (OECD, 2022).

The comparative analysis highlights that the cybersecurity governance framework in Saudi Arabia has aligned with leading international standards, while remaining flexible enough to address country-specific regulatory concerns. Further harmonization of governance, data protection, incident reporting, and third-party risk management regulations will increase legal certainty, institutional resilience, and the security of digital transactions.

7. Implications

7.1 Theoretical Implications

This study contributes to the existing legal scholarship on cybersecurity governance by providing a comprehensive perspective on cybersecurity as a legal and governance body, not just a technical security function, that includes institutional accountability, regulatory compliance, cyber risk management, and data protection. The study integrates the Saudi legal framework into internationally accepted governance principles and structures, offering a structured legal approach that establishes a connection between the principles of governance and safeguarding digital transactions. It also adds value to the literature by clarifying the meaning of the complementary relationship between cybersecurity governance, information security, and personal data protection under a unified regulatory model, which is relevant for digital environments.

7.2 Practical and Policy Implications

The results offer practical suggestions for policymakers, regulators, and digital governance organisations. The study emphasises the need to improve institutional governance by establishing clear responsibilities, board-level oversight, integrating cyber risk management, and maintaining ongoing regulatory compliance. It also highlights the importance of increased coordination between regulatory bodies in Saudi Arabia, regular auditing of the security controls to incorporate new technologies, and ongoing adherence to international standards. The measures can reinforce trust in digital transactions, make the regulation more effective, and strengthen the resilience of digital transactions in both public and private sectors.

8. Limitations and Future Research

8.1 Limitations

This study is doctrinal in nature and is mainly based on the analysis of Saudi legislation, regulatory frameworks, and internationally recognized cybersecurity standards. It does not involve empirical investigation using surveys, interviews, case studies, or quantitative analysis of institutional cybersecurity practices. In addition, the comparative analysis does not conduct a comprehensive comparison of various national legal systems, but rather analyzes the most significant international governance systems. Therefore, this research should be interpreted as normative legal research, not as an empirical evaluation.

8.2 Future Research

This study could help future research by conducting empirical analysis of the implementation of cybersecurity governance in the specific sectors of Saudi Arabia, such as financial services, healthcare, critical infrastructure, and e-commerce. Additional insights could be gained from comparative studies of the regulation of digital platforms between the countries of the GCC and other leading digital economies. Future studies could also cover novel legal issues with AI, cloud computing, digital identity, blockchain, and multi-jurisdictional data governance, aiding the ongoing advancement of cybersecurity laws and digital transaction regulations.

9. Conclusion

Cybersecurity governance has become one of the fundamental pillars underpinning the success of digital transactions and the sustainability of the digital economy. With the rapid increase in digital transformation, the process of data protection has evolved from a purely technical nature to now involve legal, regulatory, and institutional responsibilities of organizations, regulators, and senior management. This shift entails governance frameworks that need to bring risk management, compliance, operational control, and legal liability together to ensure trust in the digital space.

The study showed how Saudi Arabia has developed an effective regulatory framework by combining legislation, national cybersecurity regulations, and sectoral governance requirements. Furthermore, the comparative study reveals high levels of consistency between the regulatory system of Saudi Arabia and leading international standards of governance, risk management, business continuity, and data protection, with the possibility for further regulatory improvements as digital technologies continue to develop.

In conclusion, the effectiveness of cybersecurity governance does not depend on the amount of legislation and sanctions but on the combination of governance, compliance, cyber risk management, operational controls, and legal liability in a regulatory system. Such an integrated approach helps build digital trust, enhance organizational resilience, and offers a sustainable legal basis for safe digital transactions in an increasingly interconnected economy.

REFERENCES

1. Al-Baghdadi, M. (2021). *The Economics of Cybersecurity in the Banking Sector* [in Arabic].
2. Al-Marri, R. M. (2024). Cybersecurity and the Protection of Electronic Systems [in Arabic]. *Journal of Legal and Economic Studies*.
3. Al-Samhan, M. (2020). Cybersecurity requirements for administrative information systems [in Arabic]. *Journal of the College of Education*.
4. Al-Shammari, S. M., & Ismail, Z. M. A. (2020). Cybersecurity as a new pillar in Iraqi strategy [in Arabic]. *Journal of Political Issues*, 62.
5. Al-Tayyar, H. b. S. (2020). Cybersecurity from the perspective of the objectives of Islamic law: A foundational study [in Arabic]. *Journal of Taif University for Humanities*.
6. Anti-Cyber Crime Law, issued by Royal Decree No. M/17, dated 8/3/1428 AH (26 March 2007).
7. Capital Market Authority. (2023). *Cybersecurity Guidelines for Capital Market Institutions*.
8. Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*.
9. E-Commerce Law, issued by Royal Decree No. M/126, dated 7/11/1440 AH.
10. Electronic Transactions Law, issued by Royal Decree No. M/18, dated 8/3/1428 AH.
11. European Parliament & Council. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation—GDPR)*.
12. Hegazy, A. B. (2020). *Combating Computer and Internet Crimes under the Model Arab Law* [in Arabic].
13. International Organization for Standardization. (2018). *ISO 31000:2018 Risk management — Guidelines*. Geneva: ISO.
14. International Organization for Standardization. (2019). *ISO/IEC 27701:2019 Security Techniques—Privacy Information Management*. ISO.
15. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*. ISO.
16. International Telecommunication Union. (2024). *Global Cybersecurity Index*.
17. Jaballah, A. M. A. (2022). *Means of Cybersecurity Protection: A Foundational Jurisprudential Study Compared with Contemporary Systems* [in Arabic].
18. Khalil, H. M. (2008). *The Criminal Aspects of Cybercrimes* [in Arabic].
19. Kingdom of Saudi Arabia. (2016). *Saudi Vision 2030*. Riyadh: Kingdom of Saudi Arabia.
20. National Cybersecurity Authority. (2018). *Essential Cybersecurity Controls (ECC-1:2018)*.
21. National Cybersecurity Authority. (2022). *Data Cybersecurity Controls (DCC-1:2022)*. Riyadh: NCA.

22. National Institute of Standards and Technology. (2024). *Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce.
23. Organisation for Economic Co-operation and Development. (2022). *Digital Security Risk Management for Economic and Social Prosperity*.
24. Oughane, S. (2023). Cybersecurity and the stakes of digital transformation in Morocco: Conceptual foundations and legislative strategy [in Arabic]. *Al-Maarifa Journal*, 11.
25. Personal Data Protection Law, issued by Royal Decree No. M/19, dated 9/2/1443 AH, as amended by Royal Decree No. M/148, dated 5/9/1444 AH.
26. Saudi Central Bank. (2023). *Cyber Security Framework*.
27. Saudi Data and Artificial Intelligence Authority. (2023). *Executive Regulations of the Personal Data Protection Law*.
28. United Nations Conference on Trade and Development (UNCTAD). (2024). *Digital Economy Report 2024: Shaping an environmentally sustainable and inclusive digital future* (UNCTAD/DER/2024). Geneva: United Nations.
29. United Nations Office on Drugs and Crime (UNODC). (2021). *Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime*. Vienna: United Nations.
30. World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. Geneva: World Economic Forum.