International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cybersecurity Legal Framework in Saudi Arabia: A Comparative Analysis

Dr. Yussri Awad Abdalla

Director of the Legal Department, Al Fozan Holding Group, AL Khobar, Kingdom of Saudi Arabia.

Abstract

Background: In today's digital era, especially in a Vision 2030 country like the KSA, cybersecurity has turned into an integral legal and institutional duty, with increasing reliance on digital infrastructure, personal data, and electronic transactions.

Objective: In this study, the researchers aim to assess the efficiency of Saudi Arabia's legal and regulatory frameworks for cybersecurity in the protection of national infrastructures, personal rights, and the digital economy, as well as in facing new cyber risks.

Method: The research is of an analytical nature that discusses the main Saudi legislations such as the Anti-Cyber Crime Law, Personal Data Protection Law, Electronic Transactions Law, Telecommunications and Information Technology Law, and the Essential Cybersecurity Controls issued by the National Cybersecurity Authority (NCA). A comparative approach is used, utilizing international standards such as ISO/IEC 27001, ISO/IEC 27032, NIST Cybersecurity Framework, and some European regulatory models. **Findings:** The Saudi framework encompasses criminal protection, governance, risk management, compliance, and personal data protection, which enhances national security and trust in the digital environment. The roles and responsibilities are no longer limited to technical teams, but include Boards of Directors, Executive Management, and compliance teams. Due diligence and regulatory compliance are becoming a significant factor in determining liability. New technologies like artificial intelligence, cloud computing, IoT, and cross-border threats are new challenges that need constant adjustment in legislation and institutions.

Conclusion: Saudi Arabia's cybersecurity framework exhibits significant alignment with international standards and best practices. It has to be constantly updated and reinforced through regulation, tighter institutional compliance, and development of a legal and cybersecurity culture that favours a digital transformation and sustainable development.

Keywords: Cybersecurity; Cyberspace; National Cybersecurity Authority; Personal Data Protection; Cybercrime; Cybersecurity Governance; Risk Management; Regulatory Compliance; Saudi Legal System

I. General Introduction

In today's state, cyberspace is a legal space of its own with at least the same importance as the traditional spaces that have been regulated by law for a long time. The current landscape of human, economic, and administrative activity is one that is now defined by an interconnected digital infrastructure that supports government services, personal information, financial transactions, critical infrastructure, e-commerce, telecommunications, banking, education, health, media, and supply chains. Cybersecurity, in turn, is no longer a purely technical issue involving the protection of networks and systems, but also one of a legal,

sovereign, and regulatory nature, related to national security, the protection of rights, the stability of the digital economy, the security of public installations, and the continuity of businesses.

This importance is amplified in the Kingdom of Saudi Arabia (KSA) by the widespread digital transformation underway as part of Vision 2030, in which digital services have become integral to public administration and economic activity. The Saudi legislator has thus created a multi-layered legal and regulatory framework, from criminalization and punishment under the Anti-Cyber Crime Law, to regulation and governance via the National Cybersecurity Authority and its controls, to personal data protection, provided by the Personal Data Protection Law and its implementing regulations, to digital infrastructure, telecommunications and information technology, regulated by the Telecommunications and Information Technology Law (Kingdom of Saudi Arabia, 2007; Kingdom of Saudi Arabia, 2022; Kingdom of Saudi Arabia, 2022a; Kingdom of Saudi Arabia, 2022b).

The National Cybersecurity Authority's Essential Cybersecurity Controls (ECC-2:2024) validate their intent to enhance Cybersecurity at the national level and protect the information and technical resources of national organizations (National Cybersecurity Authority, 2024).

There is a focus on the importance of studying this framework because cybersecurity is no longer just about what takes place after an attack or crime; it has a logic of prevention, so that public and private actors have obligations related to governance, risk management, data protection, incident response, business continuity, and compliance with national controls. This change puts cybersecurity on the list of "statutory obligations" and not "optional technical practice" and imposes civil, criminal, and administrative liability in the event of a breach.

Research Gap and Contribution: Past research on Saudi cybersecurity regulation has been mostly on a law-by-law basis (e.g., the Anti-Cyber Crime Law, the Personal Data Protection Law) or on a technical level (e.g., cyber protection). They have not taken the time to sufficiently explore how these laws fit into a complete legal framework, nor how well they fit into international frameworks like ISO/IEC 27001, ISO/IEC 27032, and the NIST Cybersecurity Framework. This study fills that gap by combining a comprehensive comparison of the Saudi framework with the leading international approaches and the analysis of the Saudi framework as an integrated system of criminal law, regulatory compliance, governance, and liability. Its innovation is in revealing how the Saudi Arabia model transcends punitive regulation to preventive governance, institutional responsibility, and risk management, thus providing a unique legal perspective on cybersecurity in the context of Vision 2030 (NIST, 2024).

Accordingly, this research sees cybersecurity not as a technical science, but rather as a legal and legislative topic that encompasses three interconnected areas: preventive protection, criminalization and punishment, and governance, compliance and liability.

II. Significance of the Research

The significance of this research stems from several interconnected considerations. First, cyberspace has become an intangible facility on which the state's public services and economy depend, such that its disruption or breach may produce effects extending beyond technical loss to the disruption of public services, the interruption of financial transactions, the violation of privacy, and threats to national security. Second, modern legislation no longer views cybersecurity merely as an internal technical obligation, but as a legal duty requiring regulated entities to build a system of governance, risk management, and compliance.

Third, the Kingdom of Saudi Arabia is witnessing rapid legislative and regulatory development in this field through the continuous updating of national controls, the integration of related laws, and the linkage of cybersecurity to personal data protection and to the regulation of telecommunications, information technology, and cybercrime. This makes the study of the Saudi legal framework of both scholarly and practical importance, as it reveals the extent of this framework's capacity to address emerging cyber risks and its degree of consistency with international standards such as ISO/IEC 27001, ISO/IEC 27032, and international governance and risk-management frameworks.

III. Research Problem

The research problem derives from the fact that cyberspace is a cross-border and fast-changing multi-actor space that is intricately intertwined with risk; however, the legal rules are usually formulated within the confines of a specific territory and institution. This tension leads to questions about the sufficiency of the Saudi legal and legislative system to protect the security of cyberspace and its ability to integrate preventive protection with criminalization and punishment, institutional compliance and personal data protection, as well as the system's capacity to stand up to future challenges such as artificial intelligence, Cloud Computing, Internet of Things and cross-border attacks.

To say that the Kingdom has no legal texts is not a problem; the Kingdom has a variety of laws and controls, the problem is that these texts are not unified and are not able to create effective legal protection. For this study, effectiveness is defined as the consistency of the statutory provisions, their practical enforceability, the extent of institutional compliance with national control measures, the level of protection of the individual and of their data, and the level of adaptation of the framework to new technologies. Through this application, the study aims to identify whether Saudi Arabia's cybersecurity strategy is comprehensive from a theoretical perspective and is effectively implemented to maintain the level of trust in the cyber domain and safeguard Saudi Arabia's national interests against the ongoing technological challenges.

IV. Research Questions

The central question of this study is: How effective is the Saudi legal and legislative system for facing cyber risks and safeguarding public and private rights and interests? Effectiveness refers to how well the law is coherent, enforceable, institutionally compliant, responsive in the event of an incident, provides protection of rights, and is flexible to new technologies.

Several sub-questions arise from this central question. Cyberspace, its security and safety, legally conceived, and how do they impact liability and governance? What are the statutory underpinnings of the protection of cyberspace in the Kingdom, and how are the Anti-Cyber Crime Law, Personal Data Protection Law, Telecommunication and Information Technology Law, and the National Cybersecurity Authority's controls integrated? What are the legal consequences of non-compliance with cybersecurity obligations, and what is the devolution of duties between the criminal, civil, contractual and regulatory fields? What challenges lie ahead for the Saudi framework, especially regarding artificial intelligence, cloud, IoT, and attacks from foreign nations? Finally, how consistent is the Saudi model with international standards, such as ISO/IEC 27001, ISO/IEC 27032, the NIST Cybersecurity Framework and European approaches?

V. Research Objectives

This study has three goals. First, to create a conceptual and legal basis for the security of cyberspace, to define its meaning and its implications for liability, governance and rights. Second, to examine and understand the Saudi legislative landscape on cybersecurity, and the incorporation of criminal law, regulatory compliance, governance and personal data protection. Third, to evaluate the effectiveness of the statutory rules and regulatory controls in meeting cyber risks and their strengths and gaps, and finally to put forward some legal and regulatory recommendations to make them more effective.

In doing so, the study aims to present how Saudi Arabia's cybersecurity framework is shifting from a punitive regulatory approach to a preventive one of governance, institutional responsibility, and risk management; and to place the Saudi model in the international context of standards and best practices.

VI. Research Methodology

In the present study, three methods are used, namely the analytical, comparative, and descriptive. An analytical approach is used to analyze the pertinent Saudi statutory instruments such as the Anti-Cyber Crime Law, Personal Data Protection Law, Electronic Transactions Law, Telecommunications and Information Technology Law, and Essential Cybersecurity Controls issued by the National Cybersecurity Authority. The descriptive method is used to present the basic principles, liabilities, and dangers, but without going into the technical details that would be superfluous to understanding the legal impact.

The study's contribution is based on the comparative approach. It comprehensively compares the Saudi framework with top global standards and governance models. The standard chosen was ISO/IEC 27001, which is the most widely adopted global standard for information security management systems (ISMS) that focuses on governance, risk assessment, and compliance. The selection of ISO/IEC 27032 was motivated by the fact that it specifically covers cybersecurity in the wider context of cyberspace, connecting the technical aspects of cybersecurity protection with the responsibilities of the stakeholders. The NIST Cybersecurity Framework was added because of its widespread popularity in the United States and the fact that it breaks down the process of cybersecurity into easily identifiable categories—identify, protect, detect, respond, and recover—that can serve as a baseline for institutional implementation. Selected European approaches were taken into consideration since they emphasize data protection, accountability, and cross-border regulation cooperation, for example within the General Data Protection Regulation (GDPR) and the related cybersecurity directives (ISO, 2012, 2022, 2023; NIST, 2018, 2020, 2024; European Parliament, 2016, 2022).

The comparison is based on the following criteria: governance structure, risk-management mechanisms, incident-response procedures, data-protection obligations, accountability frameworks, safeguarding of critical infrastructure, adaptability to new technologies, and cooperation with other countries. Where Saudi provisions are similar in substance or principle to those of the international standards, the similarities are highlighted, and where obligations are less developed, less enforceable, or have not yet been adapted to the new technological challenges, gaps are noted. This transparent framework not only makes the comparative analysis descriptive but also evaluative, outlining both the good practices of Saudi regulation and the aspects that could be improved.

VII. Literature Review

The regulation of cybersecurity has been a subject of increasing scholarly interest globally, with studies on the legal, technical, and institutional aspects. International scholarship has made it clear that the

governance, risk management, compliance, and incident response aspects of a cybersecurity framework should not be neglected and must be woven into effective frameworks, alongside punitive criminal law. ISO/IEC 27001 and ISO/IEC 27032 studies reiterate the need for structured governance and stakeholder responsibility, and a review of the NIST Cybersecurity Framework talks about how it is practical and institutional implementation-focused, based on five domains: identify, protect, detect, respond, and recover (ISO, 2022; ISO, 2012; NIST, 2024; Von Solms & Van Niekerk, 2013). In European scholarship, under the General Data Protection Regulation (GDPR) and other related Directives, accountability and cross-border cooperation are key tenets of cybersecurity law, as is the protection of personal data (European Parliament & Council, 2016; European Parliament & Council, 2022).

In the Saudi context, existing studies have focused primarily on individual laws, such as the Anti-Cyber Crime Law or the Personal Data Protection Law, without considering the wider picture. These studies have yielded interesting insights into criminal liability and data-protection obligations, without properly analyzing the interplay of various laws and regulatory instruments in establishing a national framework that is coherent overall. Nor have they made a detailed comparison between Saudi regulation and international standards to understand the consistency, strengths and limitations of Saudi regulation. There also has been scholarly debate about the effectiveness of Saudi enforcement structures: some scholars have stressed the Saudi improvements in institutional governance, and others have stressed the lack of practical enforcement and compliance (Al-Harbi, 2023; Al-Shammari, 2023; Al-Otaibi, 2022; Al-Mutairi, 2023).

There are thus several gaps in the existing literature. Firstly, the incorporation of Saudi laws into a comprehensive cybersecurity framework is not adequately analyzed. Second, few studies have mapped the Saudi provisions in comparison with ISO or NIST or European approaches. Third, the effect of Saudi regulation (enforceability, institutional compliance and adaptability to new technologies) has not been demonstrated empirically.

This study is a contribution to the literature that fills in these gaps. It considers Saudi cybersecurity regulation as a whole system, including criminal law, governance, compliance, and liability, and assesses it based on the following criteria: Coherence, Enforceability, Risk Management, Incident Response, Rights Protection, and Adaptability. It also places the Saudi model in terms of the international context, with a structured comparison to ISO/IEC 27001, ISO/IEC 27032, NIST, and European approaches. This helps in the academic discourse regarding cybersecurity law and in the creation of regulations that support Saudi Arabia's digital transformation in accordance with Vision 2030 (ISO, 2022; ISO, 2012).

VIII. Conceptual Framework

The basic premise of this piece of research is that cyberspace, cybersecurity, and the safety of cyberspace are legal concepts and not only technical concepts. Cyberspace extends beyond the Internet to a domain of functioning legal, economic, and social relationships, created by digital infrastructure. Under the concept of Cyberspace as a sovereign legal space, "incidents" are not just techno-legal but legal facts with criminal, civil, and regulatory implications.

Cybersecurity, in turn, is the collection of legal, regulatory, and institutional arrangements put in place to safeguard confidentiality, integrity, and availability. The implications of each are unique: Confidentiality breaches could lead to civil damages or criminal penalties for unauthorized disclosure; integrity breaches could lead to contractual liability or regulatory sanctions for tampering with data; and the availability of data or services could result in liability for the failure to ensure that the service is available (Pfleeger &

Pfleeger, 2015; Schneier, 2015). So, cybersecurity is not just a technical matter anymore; it's a statutory requirement that affects boards of directors, compliance officers, and service providers (Brotby, 2012; Whitman & Mattord, 2022).

Security in cyberspace is not just about preventing threats, but also about cyberspace being trusted and safe to use for legitimate purposes. This concept has a direct impact on governance and rights—there should be measures in place to prevent public utilities, financial systems and individual information from being compromised, and regulators should enforce compliance and ensure the digital public interest is safeguarded. Safety therefore not only means the number of attacks prevented, but also the ability of the legal system to manage risk, minimize harm and defend rights.

Lastly, it helps define the scope of liability by differentiating between cybersecurity and cybercrime (Brenner, 2010; Von Solms & Van Niekerk, 2013). Cybercrime is a term that refers to the criminal acts that are prohibited by law, and cybersecurity is a term that encompasses the entire cyber-related, preventive, and regulatory framework. This separation allows one not just to hold the attacker liable, but to examine if institutions provided adequate diligence, control, and protection of data. In this manner, the conceptual framework is directly linked to governance, regulation, and rights protection, which then serves as a basis for the subsequent legal analysis.

IX. Analysis of the Saudi Legal Framework

Saudi Arabia's cybersecurity regulation is based on several complementary instruments, which make up an integrated system. The Anti-Cyber Crime Law introduces the criminal aspect, in that it defines the offenses of unauthorized entry, data theft, and disruption of a system, and sets penalties for violations of rights and the public interest. It is effective because of the clarity of its deterrence and legal certainty. But the problem is that it is reactive, that it is only used after harm has been done, and that it does not aim at governance. The challenges in enforcement also extend to the ability to present digital evidence and pinpoint the actual perpetrators of crimes in cross-border cases, highlighting the need for additional regulatory efforts (Kingdom of Saudi Arabia, 2007; Al-Gamal, 2021).

The Personal Data Protection Law (PDPL) is at the core of preventive cybersecurity and sets the standards of responsibility for data controllers in terms of data processing, confidentiality and lawful disclosure. Its major advantage is that it is aligned with the international trend in data protection, including GDPR, and enforceable from September 2024 onwards. However, the difficulty for private companies, particularly small and medium companies, to comply, and the absence of guidance regarding cross-border data transfers, are its drawbacks. The PDPL's connection to the Anti-Cyber Crime Law is complementary, but the interaction between the two needs to be carefully coordinated, as the same conduct could lead to criminal liability for data misuse, and regulatory liability for failing to protect the data (Kingdom of Saudi Arabia, 2022; SDAIA, 2022; Al-Khudairi, 2022; Al-Qahtani, 2024).

The Electronic Transactions Law is the source of the legal authority to trust in e-transactions, electronic signatures, contracts and records. It is strong regarding safe e-commerce and economic transactions. It is a problem, however, that it is more a matter of transactional validity than systemic cybersecurity and relies on the strength of technical standards and institutional supervision. This also has relevance with PDPL, as many secure transactions may contain sensitive personal information, which means there needs to be a balance between the commercial value of the transaction and the protection of the data (Kingdom of Saudi Arabia, 2007a; UNCITRAL, 1996, 2001).

The Telecommunications and Information Technology Law extends control beyond the traditional telecommunications to digital services and infrastructure. Its strength is the awareness of the convergence between telecommunications, IT and digital content, and a modernization of the regulatory scope. However, it is still very general, and there are issues such as cloud services, IoT devices and digital platforms for which it needs sector-specific guidance to be put into practice. It shares some common ground with the PDPL and Anti-Cyber Crime Law, which indicates a requirement for integrated compliance mechanisms to prevent this fragmentation (Kingdom of Saudi Arabia, 2022b; CST (2023).

Finally, the control framework, the National Cybersecurity Authority (NCA) controls, particularly the Essential Cybersecurity Controls (ECC-2:2024), provide a governance framework to prevent this. They are good at providing compulsory requirements for institutions in the areas of asset management, incident response, and business continuity. The weakness is in the difficulty of achieving adherence to the institutions across the different sectors, particularly when technical capacity is not equal. Their connection with statutory laws is of critical importance: legislation determines liability, and NCA controls determine how to act so that statutory laws can be fulfilled (National Cybersecurity Authority, 2024; National Cybersecurity Authority, 2022).

These tools illustrate that Saudi Arabia is moving away from a reactive cybersecurity approach and toward a more "governance-led" approach for cybersecurity. However, there are still challenges due to overlaps of laws, loopholes in enforcement, and complexity of compliance. However, if these are to be addressed, they need to be continuously improved legislatively, through improved institutional capacity, and through improved integration of the criminal, regulatory and governance elements.

X. Legal Liability

Cybersecurity liability in Saudi Arabia is not limited to the criminal liability of perpetrators, but also includes civil, contractual and regulatory aspects. This larger context is because violations of confidentiality, integrity, or availability could cause harm to the individuals involved, could cause disruption to services, or could cause damage to the trust in the digital economy without being directly attributable to any criminal act (Al-Otaibi, 2022; Sharaf, 2020).

The liability for criminal acts could be based on the Anti-Cyber Crime Law, which criminalizes system interference, data theft, and access violations. Civil liability will be enforced in cases of damage to persons or customers, including financial damage caused by a data breach. Contractual liability arises when service providers or system operators are unable to provide the level of protection agreed, and could be liable for a breach of contract claim. Regulatory liability is considered to occur when institutions do not meet the obligations of required controls, including the Personal Data Protection Law and the Essential Cybersecurity Controls published by the National Cybersecurity Authority (Al-Otaibi, 2022; Sharaf, 2020).

Through examples, the boundaries of liability of various actors can be clarified. If there is improper security, a system owner could be held liable for unauthorized access even if another person is charged with the crime. A service provider could be held contractually liable for downtime because of a cyber incident that results in violation of service-level agreements. The data processor could be liable under regulations if personal data is not processed in accordance with the requirements of PDPL. Senior management and boards of directors may be held liable under governance regulations for neglecting to be diligent in their supervision of compliance with cybersecurity regulations (Al-Mutairi, 2023; Brotby, 2012; Whitman & Mattord, 2022).

Statutory obligations and consequences of liability are demonstrated through concrete cases. As an example, if a financial institution is the victim of a ransomware attack, it could have a claim against the attacker under criminal law, but could also be subject to regulatory sanctions if it failed to take the required measures during the incident response and civil claims if users' transactions were hampered. Likewise, if a cloud service provider is breached, then it could be held liable under contract law to its customers, and could also be subject to regulatory investigation for poor risk management.

This multi-layered scheme indicates that liability under the Saudi cybersecurity law isn't limited to punishing third parties but also to assessing the extent to which institutions themselves met their duties under the law. Due diligence and compliance requirements are the focus of the argument, and the consequences of liability will hinge on whether preventive measures, reporting systems, and governance requirements are met. This will ensure that statutory requirements and accountability are tied together, making cybersecurity a shared legal responsibility in the digital arena.

XI. Emerging Technologies

New technologies pose complex legal challenges, which put Saudi Arabia's cybersecurity framework under strain. The existing framework applies to criminal law, regulatory compliance and governance, but emerging technologies add complications of liability, governance and enforcement that are beyond the scope of existing solutions.

This is the case for artificial intelligence (AI). Cyberattacks can be automated and use AI to create deep-fake identity frauds, making it harder to attribute responsibility. In the case of self-acting AI systems, the issue of liability under the Anti-Cyber Crime Law becomes complicated: who is liable – the programmer, the entity that deployed the system, or the owner of the system? This situation raises the question of statutory clarity of accountability when there is an indirect or concealed human intention (Goodman, 2015; Singer & Friedman, 2014).

Questions of jurisdiction and contractual liability arise with cloud computing. The breach could happen in a data center in a different country, and it is not clear which law applies to the incident and how responsibility would be split between the cloud providers and the client institutions. For instance, if a cloud provider fails to implement proper encryption, the responsibility could not only be contractual but also regulatory — and liable to sanctions under the Personal Data Protection Law (Lessig, 2006; Solove, 2021).

Internet of Things (IoT) brings vulnerabilities to the daily lives of people, from smart meters to medical appliances. If an IoT device is compromised, it could put critical infrastructure at risk or pose a danger to public safety. Available Saudi laws tackle unauthorized access and misuse of data but not yet specifically for IoT manufacturers and service providers. This gap begs questions as to whom should be liable: device producers, network operators, or end-users (Singer & Friedman, 2014; ENISA, 2023; Al-Bassiouni, 2022).

Existing legal frameworks are challenged too by big data analytics and automated decision-making. Potential liability under PDPL may exist if an algorithm that processes personal data has discriminatory effects or infringes on privacy. However, there must be mechanisms to enforce regulation and ensure transparency in algorithms — which is still in early stages in Saudi Arabia (Solove, 2021).

Lastly, there are risks of third-party incidents in digital supply chains. The breaching of one vendor or subcontractor in a cyber-attack could endanger the security of an entire enterprise. With current Saudi controls focusing on institutional compliance, they have yet to completely tackle the issue of allocation of

liability along complex value chains. For example, if a supplier doesn't meet the cybersecurity standards, the contracting entity may be liable for lack of due diligence (ENISA, 2023).

These scenarios illustrate that although Saudi Arabia's framework has advanced, this has to be constantly adapted. New laws are needed, as are guidance for individual sectors and increased international collaboration, since new technologies are eroding the traditional lines of liability, jurisdiction and governance.

XII. International Comparison

Saudi Arabia's cybersecurity framework should not be viewed merely as a single entity, but rather as a combination of several distinct types of international instruments against which it may be measured. Statutory obligations include binding legislation, including the Personal Data Protection Law and the Telecommunications and Information Technology Law. Institutions are subject to several mandatory operational standards because of regulatory controls, including the Essential Cybersecurity Controls (ECC-2:2024) published by the National Cybersecurity Authority (NCA). International standards like ISO/IEC 27001 and ISO/IEC 27032 are voluntary and widely used, while governance frameworks like the NIST Cybersecurity Framework offer a structured set of domains for institutional implementation, but do not have a legal mandate (NIST, 2024).

The Saudi model is quite consistent with these international approaches in aspects of governance, risk management, compliance, and incident response, among others. But this consistency must be established provision-by-provision and domain-by-domain. This comparative table shows areas of alignment, areas of partial alignment, and areas of gaps (**Table 1**).

Table 1. Comparative Table: Saudi Framework vs. International Standards.

Domain	Saudi Provisions	ISO/IEC 27001 & 27032	NIST Framework	EU/GDPR & Directives	Alignment
Governance	NCA governance controls; Telecom & IT Law	Governance structures for ISMS	Identify function (roles, responsibilities)	GDPR accountability principle	Strong alignment
Risk Management	ECC-2:2024 risk assessment requirements	Risk assessment & treatment	Identify & Protect domains	GDPR risk-based approach	Strong alignment
Incident Response	ECC-2:2024 incident reporting; Anti-Cyber Crime Law	Incident response planning	Respond & Recover domains	EU NIS Directive incident reporting	Strong alignment
Data Protection	Personal Data	ISO/IEC 27001	Protect domain	GDPR data protection obligations	Strong alignment

	Protection Law	confidentiality controls			
Accountability	PDPL duties of controllers; board responsibility	ISO/IEC 27032 stakeholder roles	Governance emphasis	GDPR accountability principle	Strong alignment
Critical Infrastructure	Telecom & IT Law; NCA sectoral controls	Sector-specific ISMS extensions	Protect domain	EU NIS Directive	Partial alignment (sectoral guidance still developing)
Emerging Technologies	Conceptual recognition in ECC-2:2024	Limited coverage	Adaptive guidance	Ongoing EU AI Act proposals	Gap (requires statutory development)
International Cooperation	General policy statements; limited treaties	Encouraged but voluntary	Not binding	GDPR cross-border transfer rules	Gap (cross-border enforcement mechanisms limited)

The structured comparison demonstrates that Saudi Arabia's framework is closely aligned to international standards in the areas of governance, risk management, incident response, data protection and accountability. In the case of critical infrastructure, regulation is still industry-specific and partially aligned. There is still a lack of adaptability to new technologies and mechanisms for international cooperation, such as cross-border enforcement and data transfers.

The study shows that the Saudi model is largely aligned with international best practices, addressing the key distinctions between binding legislation, regulatory control, voluntary standards and governance frameworks, and indicates where there is scope for further enhancement to ensure the continued effectiveness of the Saudi model in the rapidly changing digital landscape (Kingdom of Saudi Arabia, 2022; European Parliament, 2016).

XIII. Conclusion

This study aimed to assess the effectiveness of Saudi Arabia's cybersecurity law in addressing cyber risks and safeguarding rights and interests. Evaluations were made regarding the legal coherence, enforceability, institutional compliance, risk management, incident response, rights protections, and adaptability to new technologies.

The results show that Saudi regulation has evolved to encompass a holistic approach, shifting from a punitive criminal nature to one of prevention, governance, risk management and compliance. The Anti-Cyber Crime Law offers deterrence and criminal liability, and the Personal Data Protection Law sets out to prevent and imposes obligations in line with international data-protection trends. The Electronic Transactions Law guarantees digital commerce and the Telecommunications and IT Law modernizes infrastructure and services regulation. The Essential Controls operationalize governance and compliance

by the National Cybersecurity Authority. These instruments demonstrate legal coherence and good institutional underpinning.

Meanwhile, the study proves that effectiveness is based on implementation. Digital evidence remains a challenge to prove, as well as ensuring a uniform response at the institutional level, and adjusting to newer technologies like AI, IoT, and cloud computing. In comparison to ISO, NIST and EU guidelines, there is significant consistency with the international frameworks in governance, risk management and data protection; partial consistency in critical infrastructure regulation and a lack of adaptability and international cooperation.

Finally, while Saudi Arabia's overall cybersecurity framework is advanced and largely in line with international standards, its ongoing effectiveness will be supported by ongoing refinement of legislation, enhanced institutional supervision and the incorporation of mechanisms to respond to technological evolution and cross-border risks.

XIV. Recommendations

There are a series of prioritized measures that are needed to enhance Saudi Arabia's cybersecurity framework. Legislation needs to be updated to account for new technologies and to have a clear understanding of liability in relation to AI-generated attacks, IoT vulnerabilities, and cloud breaches; legislators and the National Cybersecurity Authority (NCA) need to ensure that the rules and regulations are also updated accordingly. This will allow for better accountability and be more flexible with technology. Secondly, the NCA and industry regulators should promote sector-specific guidance for cybersecurity, which would then set out industry-specific compliance requirements for finance, healthcare, energy, and telecom, etc., to give better protection of critical infrastructure and minimize regulatory fragmentation. Third, corporate boards and compliance officers should be more active in oversight, to increase accountability and institutional compliance, through governance reporting and due-diligence assessment. Fourth, the NCA should conduct regular cybersecurity maturity assessments of regulated institutions, based on ISO and NIST standards, to gauge maturity in risk management and incident response. Finally, contracting entities, vendors and regulators need to ensure the security of digital supply chains by implementing model technology contracts that include a cybersecurity clause, minimizing third-party risks and defining liability. Sixth, strengthening threat-information sharing via national platforms where cyber-threat intelligence can be shared in real-time can help critical infrastructure operators, the NCA, and the private sector in detecting cyber-threats and responding to incidents in a coordinated manner. Finally, the judiciary, law enforcement, and NCA need to further enhance digital-evidence mechanisms through standardizing procedures for the collection, preservation, and presentation of electronic evidence, increasing enforceability, and bolstering the credibility of prosecutions.

REFERENCES

1. National Cybersecurity Authority. (2024). Essential Cybersecurity Controls (ECC 2-2024). Riyadh, Saudi Arabia.
2. Kingdom of Saudi Arabia. (2007). Anti-Cyber Crime Law, issued by Royal Decree No. M/17, dated 8/3/1428 AH.
3. Kingdom of Saudi Arabia. (2007). Electronic Transactions Law, issued by Royal Decree No. M/18, dated 8/3/1428 AH.

4. Kingdom of Saudi Arabia. (2022). 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.
5. Kingdom of Saudi Arabia. (2022). Implementing Regulation of the Personal Data Protection Law. Saudi Data and Artificial Intelligence Authority (SDAIA).
6. Kingdom of Saudi Arabia. (2022). Telecommunications and Information Technology Law, issued by Royal Decree No. M/106, dated 2/11/1443 AH.
7. National Cybersecurity Authority. (2024). Essential Cybersecurity Controls (ECC 2-2024). Riyadh, Saudi Arabia.
8. National Cybersecurity Authority. (2022). Cybersecurity Governance Framework. Riyadh, Saudi Arabia.
9. Saudi Data and Artificial Intelligence Authority. (2024). Personal Data Protection Law Implementing Regulations. Riyadh, Saudi Arabia.
10. Communications, Space and Technology Commission. (2023). Regulatory Framework for Communications and Information Technology Services. Riyadh, Saudi Arabia.
11. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva: ISO.
12. International Organization for Standardization. (2023). ISO/IEC 27002:2022 Information Security Controls. Geneva: ISO.
13. International Organization for Standardization. (2023). ISO/IEC 27005:2022 Information Security Risk Management. Geneva: ISO.
14. International Organization for Standardization. (2012). ISO/IEC 27032:2012 Guidelines for Cybersecurity. Geneva: ISO.
15. International Organization for Standardization. (2018). ISO 31000:2018 Risk Management — Guidelines. Geneva: ISO.
16. National Institute of Standards and Technology. (2024). Cybersecurity Framework (CSF 2.0). Gaithersburg, MD: U.S. Department of Commerce.
17. National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5). Gaithersburg, MD.
18. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). Gaithersburg, MD.
19. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.
20. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive). Brussels.
21. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Strasbourg.
22. United Nations Commission on International Trade Law. (1996). UNCITRAL Model Law on Electronic Commerce.
23. United Nations Commission on International Trade Law. (2001). UNCITRAL Model Law on Electronic Signatures.
24. Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. Praeger.
25. Brotby, W. K. (2012). Information Security Governance: A Practical Development and Implementation Approach. Wiley.

26. Goodman, M. (2015). Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do about It. Anchor Books.
27. Lessig, L. (2006). Code: Version 2.0. Basic Books.
28. Pfleeger, C. P., & Pfleeger, S. L. (2015). Security in Computing (5th ed.). Pearson.
29. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton.
30. Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
31. Solove, D. J. (2021). Understanding Privacy. Harvard University Press.
32. Von Solms, R., & Van Niekerk, J. (2013). From Information Security to Cybersecurity. Computers & Security, 38, 97–102.
33. Al-Bassiouni, A. H. (2022). Cybersecurity and Information Protection [in Arabic]. Cairo: Dar Al-Fikr Al-Jami'i.
34. Al-Gamal, M. E. S. (2021). Cybercrime and Criminal Liability [in Arabic]. Cairo: Dar Al-Nahda Al-Arabiya.
35. Al-Harbi, A. (2023). Cybersecurity under Saudi Law [in Arabic]. Riyadh: Maktabat Al-Qanun wal-Iqtisad.
36. Al-Khudairi, K. (2022). Personal Data Protection in Saudi Legislation [in Arabic]. Riyadh: Center for Legal Studies.
37. Al-Sanhouri, A. A. (1998). Al-Waseet fi Sharh Al-Qanun Al-Madani (The Intermediary in the Explanation of the Civil Code) [in Arabic]. Cairo: Dar Al-Nahda Al-Arabiya.
38. Sharaf, A. F. (2020). Legal Liability for Electronic Crimes [in Arabic]. Cairo: Dar Al-Jami'a Al-Jadida.
39. Bada, A., Nurse, J. R. C., & Sasse, M. A. (2019). Cybersecurity Awareness Campaigns: Why Do They Fail? arXiv.
40. ENISA. (2023). ENISA Threat Landscape 2023.
41. Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' Adherence to Information Security Policies. Information & Management, 51(2), 217–224.
42. Von Solms, B., & Von Solms, R. (2018). Cybersecurity and Information Security — What Goes Where? Information & Computer Security, 26(1), 2–9.
43. Whitman, M. E., & Mattord, H. J. (2022). The Evolution of Cybersecurity Governance. Information Systems Management.
44. Al-Shammari, F. (2023). Cybersecurity in the Kingdom of Saudi Arabia: An Analytical Study [in Arabic]. Journal of King Saud University for Law and Political Science.
45. Al-Otaibi, M. (2022). Legal Liability for Cyberattacks under Saudi Law [in Arabic]. Journal of Law, Kuwait University.
46. Al-Qahtani, A. (2024). Personal Data Protection under the New Saudi Law [in Arabic]. Arab Journal of Legal Sciences.
47. Al-Mutairi, N. (2023). Governance and Cybersecurity in Saudi Government Institutions [in Arabic]. Journal of Justice.