UNIVERSITY OF MISKOLC

Deák Ferenc Doctoral School in Law and Political Sciences

THE LEGAL GOVERNANCE OF CYBERSECURITY: A CRITICAL COMPARATIVE ANALYSIS OF THE EUROPEAN UNION AND JORDAN

PhD Thesis

Candidate

Huthaifa Albustanji

Supervisors: -

Prof. dr. Paulovics Anita

Dr. Ferenc Sántha

Acknowledgments

Every doctoral journey is, in one sense, an individual pursuit; yet no dissertation is ever truly the work of one person alone. This dissertation is the culmination of years of intellectual inquiry, perseverance, uncertainty, and growth. This journey began in Jordan and continued far from home in Hungary. Along the way, I have been fortunate to encounter people whose guidance, trust, encouragement, and kindness have shaped not only this research, but also the scholar and person I have become. It is therefore with profound gratitude that I acknowledge those who, in different ways, made this journey possible and gave meaning to the years devoted to this work.

First and foremost, I express my deepest gratitude and sincere appreciation to my esteemed supervisors, Prof. Dr. Anita Paulovics and Dr. Ferenc Sántha. Their scholarly guidance, constructive critique, and unwavering encouragement were invaluable throughout every stage of this research. I have been truly privileged to benefit from their distinguished legal expertise, intellectual rigor, and generous mentorship.

I am immensely proud to have conducted my doctoral research at the Ferenc Deák Doctoral School of Law, University of Miskolc, particularly within the Institute of Criminal Sciences. My sincere thanks go to the faculty leadership and academic staff for maintaining an intellectually stimulating and supportive environment. I also extend my heartfelt appreciation to the members of the defense and discussion committee for their valuable time, critical reading, and insightful observations that enriched this work. In addition, I wish to extend my appreciation to Dr. Zoltán Varga and Dr. Bence Udvarhelyi for their kindness, support, and collegiality during my time at the faculty.

My educational and professional foundation was built across many years and institutions. I take this opportunity to thank every teacher and professor who guided my intellectual path: from my early school years in the historic city of Al-Karak, to my formative legal education at the University of Jordan (School of Law), through my specialized judicial diploma at the Judicial Institute of Jordan, and throughout my postgraduate studies at the University of Miskolc. Each stage has contributed significantly to my scholarly and professional identity.

I owe a profound debt of gratitude to the Judicial Council of Jordan for granting me the official approval and trust to pursue and complete my doctoral studies abroad. I also extend my sincere appreciation to my esteemed fellow judges, whose camaraderie, continuous encouragement, and

support have been an enduring motivation throughout my career and research. My thanks likewise go to the distinguished lawyers and the administrative staff of the Ministry of Justice for their ongoing cooperation and respect.

I am equally grateful to my second family in Miskolc—the Arab and Islamic community—who formed an inspiring home away from home, their warmth, camaraderie, and solidarity made living abroad a truly enriching experience.

Above all, words cannot adequately express the boundless gratitude I owe to my family. My deepest thanks go to my beloved parents, whose endless prayers, unconditional love, and lifelong sacrifices have been the greatest blessing and pillar of strength in my life. I am deeply thankful to my brothers and sisters, whose unwavering support, encouragement, and pride in my endeavors accompanied me every step of the way.

Finally, my deepest appreciation and gratitude go to my beloved wife, and my dear son. To my wife: thank you in recognition of your love, devotion, and extraordinary patience in bearing the burdens of living far from home and the demands of this academic journey; your steadfastness, sacrifices, and quiet strength were my greatest refuge and support, and your unwavering presence by my side had a profound and tangible impact on realizing this achievement. And to my dear son, Rashid, whose innocent presence brought boundless joy, light, and warmth to every stage of this endeavor.

Table of Contents

Chapter I: Introduction 8
I.1 Background and Context 8
I.2 Statement of Research Problem 11
I.3 Research Aim and Objectives 13
I.3.1 Research Aim 13
I.3.2 Research Objectives 13
I.4 Research Questions 14
I.4.1 Main Research Question 14
I.4.2 Sub-Questions 14
I.5 Hypothesis 15
I.6 Research Methodology 15
I.6.1 Research Design 16
I.6.2 Research Methods 16
I.7 Literature Gap and Original Contribution 17
I.7.1 Literature Gap 17
I.7.2 Original Contribution 20
I.8 Research Resources 20
I.8.1 Primary Resources 20
I.8.2 Secondary Sources 20
I.8.3 Research Sources and Collection Method 20
I.9 Significance of the Study 21
I.10 Structure of the Study 21
Chapter II: The Legal Framework of Cybersecurity in the Digital Revolution Era 22
II.1 Cybersecurity: General Overview and Roots 22
II.1.1 Conceptual and Legal Definitions 22
II.1.2 Distinguishing Cybercrime from Cyber Incidents, Cyber Threats, and Cyberattacks 26
II.1.3 Structural and Technical Factors Driving Cyber Threats 29
II.2 Historical Legislative Foundations of Cybersecurity in the EU and Jordan 31
II.2.1. The development of Cybersecurity Legislation in the EU 31
II.2.2 Roots of Cybersecurity Legislation in Jordan 33
II.3 Chapter Conclusion 35
Chapter III: The EU Legal and Regulatory Framework for Cybersecurity 35
III.1 Core Cybersecurity Legislation 35

III.1.1 The NIS Directive 35
III.1.2 Cybersecurity Act (CSA) 39
III.1.3 NIS2 Directive 42
III.1.4 Cyber Resilience Act (CRA) 47
III.1.5 Cyber Solidarity Act 54
III.2 Complementary Cybersecurity Legislation 59
III.2.1 General Data Protection Regulations (GDPR) 59
III.2.2 Artificial Intelligence Act (AIA) 62
III.2.3. The Digital Operational Resilience Act (DORA) 66
Chapter IV: The Jordanian Legal and Regulatory Framework for Cybersecurity 68
IV.1 Core Cybersecurity Legislation 68
IV.1.1 Cybersecurity Law 68
IV.2 Complementary Cybersecurity Legislation 91
IV.2.1 Jordan's Personal Data Protection Law (PDPL) 91
IV.2.2 The Electronic Crimes Law 94
Chapter V: A Critical Comparative Assessment of Cybersecurity Governance in the EU and Jordan 97
V.1 Comparative Framework for Assessment 97
V.2 Operationalizing the Regulatory Maturity Matrix 98
V.2.1 Analytical Dimensions and Maturity Tiers 98
V.2.2 Application of the Matrix to Thematic Areas 100
V.3 Preventative Cybersecurity Mechanisms 101
V.3.1 Digital Product Certification and Conformity Assessment 101
V.3.2 Risk Management Frameworks 105
V.3.3 Security of Data Processing as a Preventative Measure 109
V.4 Reactive Cybersecurity Mechanisms (During incident) 111
V.4.1 Cyber Incident Reporting Systems 112
V.4.2 Personal Data Breach Notification 115
V.5 Post-Incident Cybersecurity Mechanisms 118
V.6 Cross-Cutting Cybersecurity Mechanisms: Toward Lifecycle-Based Governance 120
V.6.1 Continuous Vulnerability Governance and Secure Development 121
V.6.2 Lifecycle-Based Product Security Regulation 123
V.6.3 Cyber Solidarity and Systemic Resilience Governance 127
V.7 General Comparative Findings 130

Chapter VI: Practical Implementation of Cybersecurity Governance in Selected EU Member States: Implications for Jordan 135
VI.1 Transition from Comparative Assessment to Practical Implementation 135
VI.2 Diversity in the Implementation of EU Cybersecurity Legislation 137
VI.2.1 Diversity in National Transposition and Regulatory Approaches 138
VI.2.2 Diversity in Risk Management and Compliance Obligations 141
VI.2.3 Diversity in Incident Reporting Obligations and Notification Frameworks 144
VI.2.4 Diversity in CRA-Based Conformity Assessment and Cybersecurity Assurance Mechanisms 148
VI.3 Challenges and Opportunities for the Adaptation of EU Cybersecurity Governance Principles in Jordan 153
VI.3.1 Institutional and Administrative Capacity Challenges 153
VI.3.2 Regulatory Complexity and Compliance Burdens 156
VI.3.3 National and Regional Cooperation Challenges 159
VI.4 Summary of Comparative Findings Among Selected EU Member states 166
Chapter VII: Roadmap for Cybersecurity Governance Reform in Jordan 167
VII.1 Purpose and Scope of the Roadmap 167
VII.2 The Legislative Reform Agenda 168
VII.2.1 Statutory Modernization of Core Definitions and Crisis Thresholds 168
VII.2.2 Recalibrating Administrative Enforcement, Sanctions and Judicial Oversight 169
VII.2.3 Legislative Harmonization between Cybersecurity and Data Protection 170
VII.3 The Institutional Governance Agenda 171
VII.3.1 Restructuring Strategic Oversight and Council Governance 171
VII.3.2 Realignment of Judicial Police Powers in NCSC and Inspection Safeguards 171
VII.3.3 Institutional Specialization and Administrative Capacity 172
VII.4 The Policy and Regulatory Governance Agenda 172
VII.4.1 Establishing a Risk-Based Cybersecurity Management Framework 172
VII.4.2 Establishing a Phased Cybersecurity Certification Framework 175
VII.5 The Operational and Technical Capacity Reform Agenda 177
VII.5.1 Multi-Stage Incident Notification, Significance Thresholds and Bidirectional Threat Intelligence Sharing 177
VII.5.2 Integrated Cybersecurity and Data-Breach Notification 180
VII.5.3 Economic and Resource Reform 180
VII.5.4 National Coordination Reform 181
VII.5.5 Regional Coordination Reform 182

Chapter VIII: Conclusion 183
VIII.1 Research Findings 183
VIII.2 Recommendations 186
VIII.3 Limitations of the Study 188
VIII.4 Directions for Future Research 189
VIII.5 Concluding Remarks 190
LIST OF REFERENCES 190
Journal Articles 190
Books 201
Book Chapter 201
Conference proceedings 201
Master Thesis 202
Professional / Practitioner Publications 202
Statutes, Regulations, and Official Legal Acts: 202
European Union Legislation and Official Reports: 202
Jordanian Legislation: 205
Other National Legislation: 206
Judicial Decisions and Case Law: 206
Annex 1: Supervisors Evaluation and Recommendations 207
Annex 2: Researcher's Publications During Study Period (2023-2026) 209
Annex 3: AI Declaration 211

Chapter I: Introduction

I.1 Background and Context

The rapid integration of digital technologies into economic, governmental, social, and critical infrastructure systems has transformed the contemporary environment into an increasingly interconnected digital ecosystem.[1] This transformation has generated substantial opportunities for economic development, public administration, communication, and technological innovation, but it has also expanded the scale and complexity of cybersecurity risks. Cyber threats have evolved beyond isolated technical incidents into increasingly organized and interconnected forms of disruption capable of affecting information systems, digital services, critical infrastructure, businesses, and individuals across national borders.[2]

The consequences of such risks extend beyond the technical functioning of individual computer systems. Cyber incidents may disrupt critical infrastructure, interrupt commercial and governmental services, compromise personal and commercially sensitive information, generate financial losses, and undermine confidence in digital systems.[3] Their effects may therefore extend simultaneously across economic, institutional, social, and national-security dimensions. The economic consequences may include direct financial losses, operational disruption, and recovery costs, while the broader social consequences may include reduced public confidence in digital services and disruption to essential aspects of social and economic life.[4]

The expansion of these risks has consequently transformed cybersecurity from a predominantly technical concern into a significant matter of legal and institutional governance. States are increasingly required not only to criminalize unlawful conduct committed through or against information systems, but also to establish preventive regulatory obligations, institutional responsibilities, incident-response mechanisms, data-protection safeguards, product-security requirements, and mechanisms for cooperation across jurisdictions. The resulting regulatory challenge is therefore broader than the punishment of cybercrime after its occurrence. It concerns the design of legal and institutional frameworks capable of preventing, managing, responding to,

[1] SÁNTHA – ALBUSTANJI, 2025, p.220.
[2] THIWISHA – VANITHA, 2026, p.2.
[3] CREMER et al., 2022, p.699.
[4] BADA – NURSE, 2020, p.74.

and recovering from cybersecurity risks while maintaining appropriate accountability for both public authorities and private actors.

In this context, cybersecurity governance may be understood as the processes, institutional arrangements, rules, and regulatory mechanisms through which responsibilities for managing cyber risks are organized, coordinated, and held accountable.[5] As a broader governance framework, it encompasses the relationships among public authorities, regulated entities, and other relevant stakeholders in pursuing defined cybersecurity objectives. This dissertation focuses specifically on the legal governance dimension of cybersecurity, examining how law structures these relationships by allocating responsibilities, establishing enforceable obligations, defining institutional competences, and providing mechanisms of oversight and accountability. This focus provides the basis for examining how cybersecurity governance is legally constituted and operationalized in the European Union (EU) and Jordan.

The EU provides an important example of this broader development in cybersecurity governance. Rather than relying upon a single cybersecurity statute, the EU has consequently developed a multi-layered regulatory architecture comprising instruments that regulate different but interconnected aspects of cybersecurity governance, including network and information-system security, cybersecurity certification, data protection, and the security of products with digital elements. Therefore, several EU legislative instruments have been adopted for enhancing these aspects such as the General Data Protection Regulation (GDPR),[6] the Cybersecurity Act (CSA),[7] the Network and Information Security (NIS) Directive,[8] subsequently replaced by the NIS2 Directive,[9]and the Cyber Resilience Act (CRA).[10]

The development of these instruments also illustrates a significant distinction between cybersecurity governance and the traditional criminal-law response to cybercrime. The Budapest

[5] Efe – Bengshir, 2019, p.36.
[6] European Parliament and Council of the European Union, Regulation No. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
[7] European Parliament and Council of the European Union, Cybersecurity Act No. 2019/881.
[8] European Parliament and Council of the European Union, Directive No. 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).
[9] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive).
[10] European Parliament and Council of the European Union, Regulation No. 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act).

Convention on Cybercrime 2001,[11] together with its 2003 Additional Protocol,[12] provides an important international framework for the criminalization of cyber-related conduct, procedural measures, and international cooperation.

By contrast, the EU's broader cybersecurity framework incorporates preventive regulatory obligations, risk-management requirements, incident reporting, product-security obligations, institutional coordination, and resilience mechanisms. The development of this framework therefore reflects a broader shift from a predominantly reactive conception of cybersecurity toward a governance model concerned with prevention, risk management, resilience, institutional coordination, and continuous regulatory oversight.

Jordan has likewise progressively developed a domestic legal and institutional framework regulating cybersecurity and digital risks, its regulatory development has followed a different trajectory, the initial legislative response focused primarily on the criminalization of computer-related and electronic offenses through the Temporary Information Systems Crime Law No. 30 of 2010,[13] followed by the Electronic Crimes Law No. 27 of 2015[14] and subsequently the Electronic Crimes Law No. 17 of 2023.[15] The development of the Cybersecurity Law No. 16 of 2019 represented a further shift from the criminal-law treatment of cyber offenses toward the establishment of a dedicated institutional framework for cybersecurity governance.[16]

The Law established the National Cybersecurity Center (NCSC) and provided a statutory basis for national cybersecurity coordination, protection, monitoring, and incident response.[17] This development is particularly significant because it demonstrates that Jordanian cybersecurity regulation is no longer confined to the criminalization of cybercrime, but increasingly incorporates institutional, preventive, administrative, and resilience-oriented dimensions.

Despite these parallel developments, the EU and Jordan have adopted substantially different approaches to the organization and implementation of cybersecurity governance. The EU

[11] Council of Europe, Convention on Cybercrime ETS No. 185, 2001.
[12] Council of Europe, Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, 2003.
[13] Jordan, Temporary Information Systems Crime Law No. 30 of 2010.
[14] Jordan, Electronic Crimes Law No. 27 of 2015.
[15] Jordan, Electronic Crimes Law No. 17 of 2023.
[16] Jordan, Cybersecurity Law No. 16 of 2019.
[17] Ibid., Article 6.

framework has evolved through multiple interconnected legislative instruments that distribute responsibilities among European and national institutions while imposing differentiated obligations on public authorities, essential and important entities, digital service providers, manufacturers, and other market actors.

Jordan, by contrast, has developed a more centralized institutional architecture in which the NCSC occupies a prominent role in national cybersecurity coordination and oversight. The comparison is therefore not limited to whether particular cybersecurity rules exist in each jurisdiction; rather, it concerns how legal obligations are structured, which institutions are responsible for implementing and enforcing them, how risks are allocated between public and private actors, and how preventive, reactive, and resilience-oriented mechanisms are incorporated into the legal system.

I.2 Statement of Research Problem

Despite Jordan's progressive development of legislation and institutions regulating cybercrime and cybersecurity, the existence of multiple legal instruments does not, in itself, establish whether the resulting framework constitutes a sufficiently coherent, preventive, enforceable, and resilient system of cybersecurity governance. The interaction between criminal legislation, the cybersecurity regulations, data-protection legislation, electronic-transactions rules, institutional mandates, and secondary regulatory measures raises questions concerning the allocation of legal responsibilities, the scope of administrative powers, the enforceability of cybersecurity obligations, and the mechanisms available for preventing and responding to systemic cyber risks.

The central problem of this study therefore concerns the regulatory and institutional maturity of Jordan's cybersecurity governance framework. In particular, it is necessary to determine whether the existing framework adequately translates cybersecurity objectives into legally enforceable preventive obligations, proportionate risk-management requirements, effective incident-response mechanisms, institutional accountability, and mechanisms capable of regulating cybersecurity risks throughout the lifecycle of digital systems and products.

A further dimension of the problem concerns institutional design. The Jordanian cybersecurity framework assigns substantial responsibilities to the NCSC within a centralized

national governance structure.[18] This raises questions concerning the distribution of regulatory, supervisory, coordination, and enforcement functions; the relationship between cybersecurity authorities and other governmental institutions; the availability of appropriate accountability mechanisms; and the extent to which the legal framework establishes sufficiently clear boundaries between administrative cybersecurity governance and judicial or law-enforcement functions. These issues require examination of the relevant statutory provisions and cannot be resolved solely through institutional description.

The problem also extends to the preventive and risk-based character of the regulatory framework. Modern cybersecurity governance increasingly incorporates continuous risk management, organizational security obligations, incident reporting, vulnerability management, supply-chain security, product-security requirements, and lifecycle approaches. The extent to which these elements are incorporated into Jordanian law, and the degree to which they are supported by enforceable statutory or regulatory mechanisms, therefore requires systematic assessment.

A further challenge arises from the inherently cross-border character of cybersecurity. Digital infrastructure, data flows, cyber incidents, technology suppliers, and cybercrime investigations frequently extend beyond national jurisdiction. Consequently, the adequacy of a national cybersecurity framework depends not only upon domestic legislation but also upon its capacity for institutional coordination, information sharing, international cooperation, and interoperability with broader regional and international mechanisms.

The EU provides a useful comparative framework for examining these questions because its cybersecurity architecture combines multiple legislative instruments, differentiated institutional responsibilities, risk-based regulatory obligations, enforcement mechanisms, and cross-border coordination structures. However, the purpose of the comparison is not to assume that the EU framework should be directly transplanted into Jordan. Rather, the comparison seeks to determine which regulatory and institutional mechanisms may be functionally relevant to Jordan, which elements may be unsuitable because of differences in institutional and economic capacity, and how

[18] Ibid.

practical implementation experience within selected EU Member States may illuminate the conditions necessary for successful regulatory operation.

Accordingly, the research problem of this study concerns whether, and to what extent, Jordan's existing legal and institutional framework provides an adequate and coherent basis for the effective governance of contemporary cybersecurity risks throughout the lifecycle of cyber incidents, from prevention and preparedness to detection, reporting, response, investigation, recovery, and the maintenance of longer-term resilience. The study therefore examines the extent to which the applicable legal rules allocate responsibilities among relevant institutions and regulated actors, establish enforceable obligations, provide appropriate mechanisms for risk management and incident handling, and ensure effective institutional coordination and oversight. Against this background, the research further considers the extent to which the EU's legislative and institutional experience, together with the practical experience of selected Member States, may provide a basis for identifying legally and institutionally appropriate reforms for the Jordanian framework.

I.3 Research Aim and Objectives

I.3.1 Research Aim

The primary aim of this study is to critically assess and comparatively evaluate the legal and institutional governance of cybersecurity in Jordan and the EU, with particular attention to regulatory design, legal enforceability, risk management, institutional responsibility, preventive and reactive mechanisms, and practical implementation. On the basis of this comparison, the study seeks to identify context-sensitive legal and institutional reforms capable of strengthening cybersecurity governance and digital resilience in Jordan.

I.3.2 Research Objectives

1- To examine the conceptual, legal, and historical development of cybersecurity governance and distinguish its preventive and regulatory functions from the reactive criminal-law treatment of cybercrime.

2- To analyze the EU's cybersecurity legal and institutional framework, including the principal legislative instruments governing cybersecurity, data protection, network and information-system security, product security, and related regulatory mechanisms.

3- To analyze Jordan's cybersecurity legal and institutional framework, including the Cybersecurity Law, Electronic Crimes Law, Personal Data Protection Law (PDPL), and relevant institutional and regulatory arrangements.
4- To comparatively evaluate the Jordanian and EU frameworks in relation to legal bindingness, risk proportionality, enforcement, institutional capacity, private-sector responsibilities, lifecycle continuity, resilience, and operational interoperability.
5- To examine the practical implementation of EU cybersecurity legislation in selected Member States and identify institutional, administrative, technical, and economic factors affecting regulatory implementation.
6- To assess the extent to which relevant EU regulatory and institutional mechanisms may be adapted to the Jordanian context, taking account of differences in institutional capacity, regulatory structures, and economic conditions.
7- To formulate a phased and context-sensitive legal and institutional reform roadmap for strengthening cybersecurity governance in Jordan.

I.4 Research Questions

I.4.1 Main Research Question

To what extent does Jordan’s existing legal and institutional framework provide an effective basis for governing contemporary cybersecurity risks, and what legal and institutional reforms may be derived from a comparative assessment of the EU and the practical implementation experience of selected EU Member States?

I.4.2 Sub-Questions

1- What are the principal legal and institutional foundations of cybersecurity governance in Jordan and the EU, and how do their respective legal frameworks regulate the governance of cybersecurity risks throughout the incident lifecycle?
2- To what extent do the Jordanian and EU frameworks differ in the allocation of regulatory responsibilities, the bindingness and enforceability of legal obligations, risk management, institutional oversight, enforcement, private-sector responsibilities, inter-institutional cooperation, and mechanisms for maintaining cybersecurity resilience?

3- What does the implementation of EU cybersecurity legislation in selected Member States reveal about the institutional, administrative, technical, and economic conditions necessary for the effective and sustainable operation of cybersecurity regulation?
4- To what extent, and subject to what legal, institutional, and economic conditions, can elements of the EU's cybersecurity governance experience be adapted to the Jordanian context, and what reforms would be required to strengthen Jordan's cybersecurity governance without creating disproportionate regulatory or institutional burdens?

I.5 Hypothesis

The study proceeds on the proposition that Jordan's existing cybersecurity framework provides an important statutory and institutional foundation for national cybersecurity governance but remains comparatively less developed in several dimensions of preventive, risk-based, and lifecycle-oriented regulation. It is further hypothesized that greater statutory clarity, differentiated risk-based obligations, clearer institutional allocation of responsibilities, stronger enforcement and accountability mechanisms, and enhanced preventive and lifecycle requirements could improve the effectiveness and resilience of Jordan's cybersecurity governance.

The study further hypothesizes that the EU's experience provides relevant regulatory mechanisms and institutional practices from which Jordan may derive useful lessons, but that direct transplantation of EU rules would not necessarily produce equivalent outcomes because regulatory effectiveness depends upon institutional frameworks, administrative structures, technical and human capabilities, and economic situation. Accordingly, the study tests whether selective and context-sensitive adaptation, rather than wholesale legal transplantation, provides the more appropriate pathway for strengthening Jordan's cybersecurity governance.

I.6 Research Methodology

This research adopts a qualitative comparative legal methodology to critically examine the legal and institutional governance of cybersecurity in Jordan and the EU. The study combines doctrinal legal analysis with comparative and evaluative analysis in order to examine not only the content of relevant legislation but also the institutional structures, regulatory mechanisms, enforcement arrangements, and implementation conditions through which cybersecurity obligations are operationalized.

I.6.1 Research Design

The research is designed as a comparative legal study of two principal regulatory contexts: Jordan and the EU. The EU is selected as a comparative reference on account of the breadth, and institutional development of its cybersecurity regulatory framework, which provides a developed example of how legal and institutional mechanisms may be structured to address the increasingly complex risks arising from digitalization.

The comparison does not treat the EU framework as a universally applicable model, nor does it assume that greater regulatory complexity necessarily produces superior outcomes. Rather, the study examines the legal and institutional approaches adopted in each jurisdiction, considers how they respond to comparable governance challenges, and evaluates their regulatory coherence, institutional implications, and capacity to address comparable cybersecurity governance challenges.

To bridge the gap between statutory design and practical enforcement, the comparative analysis incorporates a comparative examination of national implementation practices of selected EU Member States. Evaluating how selected national jurisdictions transpose and operationalize supranational mandates helps identify administrative bottlenecks, institutional costs, and regulatory friction that may arise in the implementation of the European framework, thereby establishing a more realistic basis for assessing the viability of legal reform in Jordan.

I.6.2 Research Methods

I.6.2.1 Comparative Legal Method

The study applies a functional comparative legal method, examining how Jordanian and EU legal frameworks regulate comparable cybersecurity governance functions rather than limiting comparison to textual similarities or differences. The analysis examines the core dimensions of cybersecurity governance across the preventative, reactive, post-incident, and continuous lifecycle phases.

This functional comparison is integrated with an evaluative and normative policy analysis, utilizing a customized Regulatory Maturity Matrix, spanning statutory bindingness, institutional distribution, risk proportionality, and enforcement mechanisms. This methodological focus allows the study to distinguish mere variations in legislative drafting from substantive structural divergences in governance design.

I.6.2.2 Analytical and Evaluative Method

The comparative inquiry is integrated with an analytical and evaluative method to assess the legal coherence, institutional capacity and regulatory maturity of the Jordanian and EU frameworks. Rather than relying on static, provision-by-provision textual comparisons, this method operationalizes a customized Regulatory Maturity Matrix structured around eight qualitative benchmarks: statutory bindingness, risk proportionality, enforcement mechanisms, institutional capacity, private-sector engagement, lifecycle continuity, resilience integration, and operational interoperability.

The Matrix functions as a qualitative diagnostic tool to map formal statutory provisions across both jurisdictions onto defined levels of regulatory maturity. The Matrix is used first to identify structural differences between the two systems and second to assess whether the more developed EU mechanisms remain operationally suitable when considered against Jordanian institutional and economic conditions.

By balancing normative legal benchmarking against domestic institutional capacities, economic constraints, and compliance burdens, this evaluative method establishes the evidentiary foundation required to answer the study's central research question and formulate an actionable, context-sensitive legislative roadmap for Jordan.

I.7 Literature Gap and Original Contribution

I.7.1 Literature Gap

The existing literature on cybersecurity in Jordan has tackled a number of important aspects of the country’s emerging cybersecurity framework, including legislative development, institutional governance, organizational compliance, enforcement, coordination, and risk management. However, the existing scholarship remains predominantly focused on individual components of the Jordanian framework rather than examining its overall legal and institutional architecture through a systematic comparative legal-governance analysis.

For example, Almomani, Mehdawi and Allabadi examine the Jordanian National Cyber Security Framework from an organizational compliance perspective.[19] Their study provides a detailed analysis of the framework and develops a self-assessment tool for measuring institutional

[19] ALMOMANI et al., 2026, p.2.

compliance with the JNCSF and selected international standards. Its principal concern is therefore the assessment of organizational compliance and governance readiness, rather than the broader legal architecture through which cybersecurity responsibilities, regulatory powers, institutional relationships, enforcement mechanisms, and incident management are established and exercised.

Similarly, Bani Younes et al. examine the legislative evolution of cybersecurity in Jordan by tracing the development of Jordanian cyber-related legislation and considering its effectiveness in light of the prevalence of cybercrime and cyberattacks.[20] Their analysis identifies continuing weaknesses in the Jordanian legal framework, particularly in relation to the identification and prosecution of perpetrators. The study therefore contributes to understanding the development and effectiveness of Jordanian cyber legislation, but does not undertake a comprehensive comparative examination of Jordan's regulatory architecture against the EU's contemporary cybersecurity framework.

The study by Al Muhaisen et al. moves further toward a governance-oriented assessment by examining Cybersecurity Law No. 16 of 2019 and identifying shortcomings relating to enforcement, coordination, integration, international cooperation, and risk-based regulation.[21] This work is particularly relevant to the present research because it recognizes that Jordanian cybersecurity regulation extends beyond the criminalization of cybercrime and involves broader questions of governance and risk management. Nevertheless, its comparison with global standards remains principally evaluative and policy-oriented and does not develop a structured doctrinal comparison between the Jordanian and EU legal frameworks or examine how EU cybersecurity legislation operates through different national institutional arrangements.

Taken together, these studies demonstrate that Jordanian scholarship has already established an important body of research on cybersecurity law and governance. The gap is therefore not the absence of research on Jordanian cybersecurity, but the absence of an integrated comparative legal inquiry connecting the different dimensions of the regulatory system**.** Existing studies tend to examine legislation, organizational compliance, enforcement, or governance challenges separately. Limited attention has been given to how these elements interact within a broader legal architecture governing cybersecurity throughout the progression from preventive

[20] YOUNES et al., 2024, p.817.
[21] AL-MUHAISEN et al., 2024, p.852.

regulation and preparedness through risk management, detection, reporting, response, investigation, recovery, and longer-term resilience.

A further limitation concerns the comparative dimension. The existing Jordanian literature identified above does not provide a systematic comparison between Jordan's cybersecurity legal and institutional framework and the EU's developing body of cybersecurity legislation, nor does it examine the differences in legal bindingness, allocation of regulatory authority, institutional oversight, enforcement, private-sector obligations, regulatory continuity, and resilience through a common analytical framework. Consequently, the existing literature provides important assessments of individual aspects of Jordanian cybersecurity governance but does not sufficiently explain how the Jordanian model compares structurally with a mature multi-level regulatory system such as that of the EU.

The literature also gives limited attention to the practical implementation of EU cybersecurity legislation at Member State level as a source of comparative evidence for Jordan. This is significant because the formal content of EU legislation does not by itself determine regulatory effectiveness. Its operation is mediated by national legislative transposition, administrative structures, supervisory institutions, technical capabilities, enforcement practices, and economic conditions. Examining selected Member States therefore makes it possible to distinguish between the formal regulatory design of the EU and the conditions required for its practical operation, an issue that cannot be adequately addressed through a comparison of statutory texts alone.

Accordingly, this study addresses a threefold gap in the existing literature. First, it brings together the principal legal and institutional dimensions of Jordanian cybersecurity governance within a single analytical framework rather than examining individual statutes or compliance mechanisms in isolation. Second, it places that framework in systematic comparison with the EU's multi-level cybersecurity regulatory architecture. Third, it extends the comparison to the practical implementation experiences of selected EU Member States in order to assess the institutional and contextual conditions affecting the operation of cybersecurity regulation and, on that basis, determine which elements of the European experience may be appropriately adapted to Jordan.

I.7.2 Original Contribution

The principal original contribution of this study lies in integrating lies in bringing together, within a single comparative legal analysis, dimensions that existing Jordanian scholarship has largely examined separately. Rather than focusing primarily on the evolution of Jordanian cyber legislation, the effectiveness of individual laws, or organizational compliance with the Jordanian National Cyber Security Framework, this research examines cybersecurity governance as an integrated legal and institutional system across the full cybersecurity lifecycle, comparing Jordan with the EU and incorporating the practical implementation experience of selected EU Member States. On this basis, it develops a structured Regulatory Maturity Matrix and uses the comparative findings to formulate a context-sensitive, phased reform framework for Jordan.

I.8 Research Resources

I.8.1 Primary Resources

The primary sources consist principally of legislation, regulations, official legal instruments, judicial decisions, and relevant international and regional legal instruments. For Jordan, the analysis includes for instance the Cybersecurity Law No. 16 of 2019, the Electronic Crimes Law No. 17 of 2023 and the PDPL No. 24 of 2023. For the EU, the primary texts comprise GDPR, CSA, NIS2, CRA, DORA, AI act and the Cyber Solidarity Act.

I.8.2 Secondary Sources

The secondary legal data includes peer-reviewed academic literature, books, book chapter, comparative law treatises, specialized legal commentaries, official regulatory guidelines issued by the European Union Agency for Cybersecurity (ENISA), National Strategies from Jordan's NCSC, and reports from international organizations.

I.8.3 Research Sources and Collection Method

This study relies on a doctrinal legal research model. Data collection was executed through official, verified legal databases to ensure the authenticity and reliability of the legal materials consulted. Jordanian statutory texts and amendments were retrieved from the official Jordanian Gazette and institutional legislative portals. EU regulatory acts, directives, and preparatory instruments were obtained from the official EUR-Lex database and European Commission publication repositories. Secondary academic scholarship, treatise chapters, and international legal commentary were

compiled systematically from digital indexes, including HeinOnline, Westlaw, and Google Scholar.

I.9 Significance of the Study

This study provides distinct contributions across multiple professional and academic dimensions:

1- Legal significance: It contributes to comparative Cybersecurity Law by examining how different legal systems allocate regulatory responsibilities, establish enforceable cybersecurity obligations, and integrate preventive, reactive, and resilience-oriented mechanisms.
2- Institutional significance: It examines the relationship between cybersecurity legislation and institutional design, with particular attention to regulatory allocation, supervisory capacity, enforcement, coordination, and accountability.
3- Comparative significance: It provides a structured comparison between Jordan and the EU while recognizing that regulatory maturity must be evaluated in relation to institutional and economic context rather than through legislative volume alone.
4- Practical significance: By incorporating implementation experiences from selected EU Member States, the study identifies practical conditions that may affect the sustainability of cybersecurity regulation and uses these findings to inform context-sensitive recommendations for Jordan.
5- Policy significance: The resulting reform framework seeks to provide Jordanian policymakers with a phased approach to strengthening cybersecurity governance while taking account of institutional capacity, regulatory feasibility, and compliance burdens.

I.10 Structure of the Study

To ensure a progressive build from doctrinal foundation to practical application, this study is organized into eight interconnected chapters:

- Chapter I (Introduction): Outlines the research parameters, methodological design, literature gaps, primary hypotheses, and foundational context.
- Chapter II (The Legal Framework of Cybersecurity in the Digital Revolution Era): Evaluates the historical foundations of cyber risk, defines core legal concepts.

- Chapter III (The EU Legal and Regulatory Framework for Cybersecurity): Conducts a comprehensive doctrinal mapping of core and complementary EU cybersecurity legislation (NIS2, CRA, GDPR, AI Act, and DORA).
- Chapter IV (The Jordanian Legal and Regulatory Framework for Cybersecurity): Evaluates the domestic statutes of Jordan, critically assessing the institutional setup of the NCSC and examining complementary Laws.
- Chapter V (A Critical Comparative Assessment of Cybersecurity Legislative Principles in Jordan and the EU): Deploys a customized Regulatory Maturity Matrix to execute a structural, thematic comparison of preventive, reactive, and post-incident mechanisms in both systems.
- Chapter VI (Practical Implementation of Cybersecurity Governance in Selected EU Member States: Implications for Jordan): Analyzes the administrative fragmentation and enforcement friction encountered during Member State transposition of EU laws, identifying practical limits to legal transplantation.
- Chapter VII (Roadmap for Cybersecurity Governance Reform in Jordan): Formulates a comprehensive legislative and institutional reform agenda, systematically mapped onto Short-Term (Foundational Reforms), Medium-Term (Institutional Consolidation), and Long-Term (Advanced Governance) implementation horizons.
- Chapter VIII (Conclusion): Synthesizes the core comparative findings, identifies research limitations, and articulates future trajectories for legal scholarship in cyber governance.

Chapter II: The Legal Framework of Cybersecurity in the Digital Revolution Era

II.1 Cybersecurity: General Overview and Roots

II.1.1 Conceptual and Legal Definitions

The widespread availability of network connectivity allows individuals and organizations to engage with the global community through digital platforms. However, this connectivity also introduces exposure to potential unauthorized access from external actors. Data transmitted across multiple devices and products often encrypted, travels through networks structured in layered architectures, each presenting specific vulnerabilities. These weaknesses can be exploited, making

cyber threats against networks and interconnected products both feasible and increasingly prevalent in the online environment.[22]

In this context, cybersecurity has become a critical priority in the contemporary technological landscape. Individuals, organizations, and States are increasingly confronted with a growing spectrum of sophisticated and diverse cyber threats. These range from ransomware and phishing schemes to large-scale data breaches and targeted attacks on critical infrastructure. To effectively understand these threats, it is essential to first delineate the key legal terminologies in cyberspace, such as cybersecurity, cyber threats, and cybercrime. These definitions establish the conceptual foundation for assessing their scope and governance implications.[23]

The concept of cybersecurity has evolved both linguistically and legally, shaped by technological progress and regulatory developments across jurisdictions. The term "cyber" derives from the Greek word κυβερνητική (kybernetike), meaning "the art of steering" or "control." The modern conceptual history of cyber is commonly associated with cybernetics, a field developed by Norbert Wiener, whose 1948 work Cybernetics examined communication and control in animals and machines.[24] Complementing this, the term security refers to the protection, safeguarding, and defense of systems, information, or assets against threats, risks, or unauthorized access. [25] When combined, cybersecurity represents the integration of digital connectivity and protective governance measures to ensure the confidentiality, integrity, and availability of digital systems, networks, and data.

At the legal level, definitions of cybersecurity differ across jurisdictions. The EU, through the CSA, defines it as the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.[26] In scholarly discourse, cybersecurity is often characterized as a set of defensive techniques and security measures aimed at identifying, mitigating, and countering potential intrusions.[27]

[22] ASLAN et al. 2023, p.2.
[23] ALBUSTANJI, 2023, p.147.
[24] WIENER, 1961, p.116.
[25] WEIPPL – SCHRITTWIESER, 2024, p.397.
[26] European Parliament and Council of the European Union, Cybersecurity Act No. 2019/881, Article 2(1).
[27] MOSTAFA, 2022, p.722.

In Jordan, the Cybersecurity Law defines cybersecurity as the measures taken to protect information systems, networks, and critical infrastructure from cybersecurity incidents, and the ability to restore their functioning and continuity, whether the incidents result from unauthorized access, misuse, failure to follow security procedures, or deception leading to such breaches.[28]

The Jordanian legal definition of cybersecurity highlights its main elements, as previously mentioned, but it does more than just outline these components. From a legislative-drafting perspective, the definition could be regarded as relatively detailed because it incorporates several examples of conduct capable of giving rise to cybersecurity incidents. Therefore, including such specifics within the definition goes beyond its intended scope, as a definition should provide a concise description or brief explanation to clarify meaning. Detailed accounts of ways to circumvent cybersecurity measures fall under expanded explanation and should exist elsewhere in the statute rather than within the definition itself.

Building on this, contemporary national regulatory regimes seek to provide precise and structured definitions of cybersecurity, focusing on its core purpose of protecting information systems, networks, software, and data from unauthorized access or operational disruption. These modern governance approaches emphasize clarity and brevity, avoiding technical details to maintain a clear distinction between the statutory definition and broader administrative provisions addressing specific security controls or intrusion vectors.

Although cybersecurity establishes protective governance frameworks, the prevalence of digital offenses compels states to enact specific penal provisions categorizing unlawful acts as punishable offenses. To this extent, scholars have not reached a single, universally accepted definition of cybercrime. Some refer to it as "internet crimes," while others describe it as computer-related or information crimes.[29]

Certain legal scholars define cybercrime as a set of criminal acts involving the use of the internet, computers, or other electronic devices. In a broader sense, cybercrimes encompass a wide spectrum of illicit conduct perpetrated by individuals or groups against computers, computer-

[28] Jordan, Cybersecurity Law No. 16 of 2019. Article (2).
[29] LOTFI, 2022, p.154.

related devices, or information networks, as well as traditional crimes facilitated through the internet or information technology.[30]

The Jordanian Electronic Crimes Law does not provide a direct statutory definition of cybercrime, leaving conceptual interpretation to the judiciary. In this regard, a ruling by the Amman Court of First Instance defined electronic crimes as a set of unlawful acts carried out through electronic equipment, devices, or the internet, or as offenses proven by digital content. The ruling further emphasized that a computer may serve multiple roles: as the target of the offense, the subject matter of the crime, or the tool used to commit it.[31]

The absence of a statutory definition introduces potential inconsistencies in judicial interpretation. Incorporating a clear, precise definition of cybercrime within the penal framework would standardize judicial application, reduce ambiguity, and provide a consistent statutory basis for evaluating digital offenses. It is fundamentally the role of the legislature to establish primary legal constructs, while the judiciary's responsibility is to apply these statutory norms to concrete cases.

In the EU approach, while the Directive on attacks against information systems does not provide a precise definition of cybercrime,[32] the Budapest Convention on Cybercrime which is ratified by most EU Member States and integrated into EU legal practice, offers a better clarification on what consists cybercrime.[33] Although the Convention does not provide a single comprehensive statutory definition of 'cybercrime', it establishes a structured framework of substantive offences directed against the confidentiality, integrity, and availability of computer systems and data, together with computer-related fraud, forgery, and other offences.[34]

It is evident from these statutory frameworks that legal definitions of cybercrime remain broad. Cybercrime is recognized whenever the object or the means of the offense involves electronic systems. The means may include information systems, networks, or digital technologies, while the object may consist of individuals, commercial entities, or public networks.

---

[30] PHILLIPS et al., 2022, p.382
[31] Jordan, Amman Court of First Instance (Criminal Division, Appellate Jurisdiction), Decision No. 1050/2021, Judgement of 9 May 2021.
[32] European Parliament and Council of the European Union, Directive 2013/40 on attacks against information systems.
[33] Council of Europe, Convention on Cybercrime (ETS No. 185), 2001.
[34] Council of Europe, Convention on Cybercrime (ETS No. 185), 2001, Article 2.

Accordingly, cybercrimes can be categorized according to their relationship with digital systems into three primary types:[35]

1. Crimes against the machine: Offenses targeting the integrity of information systems directly, such as unauthorized access, system interference, and DoS/DDoS attacks.
2. Crimes using the machine: Employing digital tools to commit traditional offenses, including fraud, forgery, and financial scams.
3. Crimes in the machine: Offenses involving illicit or harmful content within digital systems, such as online harassment, hate speech, or unlawful material.

This taxonomy clarifies the target of various offenses and aids in evaluating penal provisions. However, many acts directed against information infrastructure remain insufficiently criminalized in certain jurisdictions, often being treated merely as technical anomalies, cyber threats, or cyber incidents. This distinction reveals a critical gap between penal enforcement and administrative governance, which is examined in the following section.

II.1.2 Distinguishing Cybercrime from Cyber Incidents, Cyber Threats, and Cyberattacks

The absence of standardized definitions for cybercrime, cyber threats, and cybersecurity incidents contributes to conceptual uncertainty within digital governance. Divergent legal frameworks across jurisdictions complicate regulatory enforcement, judicial coordination, and cross-border oversight.[36]

From a legal perspective, a cyber act cannot be classified as a crime unless explicitly criminalized by statute, in accordance with the principle *nullum crimen, nulla poena sine lege* (no crime and no penalty without a legal provision).[37] Accordingly, harmful cyber activity that is not recognized as an offense under existing penal legislation cannot be processed as a cybercrime. This criminal law principle highlights the necessity of establishing clear, distinct administrative terminologies for non-criminal or preventive activities in the cyber domain.

To resolve this conceptual fragmentation, contemporary legal scholarship increasingly adopts a taxonomy-based approach to cyber offenses. Scholars distinguish between three principal

[35] PHILLIPS et al., 2022, p.384.
[36] SARKAR – SHUKLA, 2024, p.4.
[37] AUSTIN, 2020, p.8.

categories: First, cyber-dependent crimes (or "true" cybercrimes), in which the computer or information system constitutes the direct target of the offense and the crime could not occur without digital infrastructure for example, illegal access (hacking) or system interference. Second, cyber-enabled or hybrid crimes, in which digital technologies play a substantial facilitating role, although the underlying offense could, in principle, be committed without a computer such as fraud, identity theft, or financial exploitation conducted through online platforms. Third, cyber-assisted crimes, in which the use of computers is incidental to traditional criminal conduct and primarily serves to expand opportunities for real-world offenses, such as criminal communications or coordination through digital networks.[38]

This taxonomy is analytically significant because it separates crimes directed against information systems from crimes that merely use digital technologies as instruments. This categorization carries direct implications for legislative drafting, jurisdictional allocation, evidentiary standards, and regulatory oversight.

However, cybercrime represents only one subset of harmful conduct in the digital environment. Not all cybersecurity incidents constitute criminal offenses, and not all cyber threats fall within the scope of criminal law.[39] Modern cybersecurity governance therefore operates on a broader regulatory plane that extends beyond penal sanctions to include administrative prevention, continuous risk management, and incident response mechanisms. It is within this broader regulatory context that the concept of a "cybersecurity incident" acquires particular governance significance.

In this context, the Jordanian Cybersecurity Law introduced the concept of a cybersecurity incident as a legal notion, defining it as "the act or attack that represents a risk to data, information, information systems, Internet, or infrastructure related thereto and requires a response to suspend or to minimize the consequences or effects thereof".[40] Similarly, the EU NIS2 Directive defines a cybersecurity incident as "an event compromising the availability, authenticity, integrity or

[38] SÁNTHA, 2024, p.33.
[39] McCormick, T.: What Counts as Cyber Crime? McCormick Law, January 2025. Available at: https://www.rbmccormicklaw.com/blog/2025/january/what-counts-as-cyber-crime-/. (Accessed 10 September 2026).
[40] Jordan, Cybersecurity Law No. 16 of 2019, Article 2.

confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems".[41]

While both definitions address harmful digital events, their scopes diverge significantly. The Jordanian definition appears narrower in formulation because it is framed around an 'act or attack' that poses a threat and requires a response, whereas the NIS2 definition focuses on the consequences of an event for the availability, authenticity, integrity, or confidentiality of data or services. The Jordanian formulation may therefore provide less explicit coverage of non-adversarial operational disruptions, such as certain forms of human error, software failure, or misconfiguration.[42]

Beyond incidents, cyber threats encompass a wider range of potential risks, including cybercrime, cyberterrorism, cyberespionage, and cyberwarfare. Cyber threats constitute a broader governance category than cyber offenses, as they extend beyond criminalized acts to include any condition or event that threatens network integrity.[43]

According to European regulations, cyber threats are defined under the EU CSA as "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons." The European definition adopts a broad, systemic perspective, encompassing both intentional and unintentional events affecting networks, information systems, and users. This supports a comprehensive, risk-based cybersecurity governance model across EU Member States. In contrast, the Jordanian Cybersecurity Law does not provide a comparable legal definition of cyber threats. The current statutory text leaves a conceptual gap regarding the primary legal definition of cyber threats.

From a comparative governance perspective, the lack of an overarching statutory baseline leaves the boundary between environmental vulnerabilities "cyber threats" and actualized, deliberate disruptions "cyberattacks" unarticulated in primary legislation.[44] Unlike cyber threats,

[41] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive). Article (6/5).
[42] KOSIŃSKI et al., 2018, p.119.
[43] OPDERBECK, 2016, p.936.
[44] ABU et al., 2018, p.371.

which represent potential risks or latent vulnerabilities, cyberattack is used to refer to an intentional hostile act directed against or through digital systems or infrastructure.

Accurate statutory taxonomy remains essential for administrative governance. Clear conceptual boundaries enable the precise allocation of administrative authority, establish objective triggers for mandatory incident reporting, shape product security standards, and guide national risk management frameworks. These conceptual distinctions provide the analytical foundation for examining the structural and technical factors that contribute to the increasing frequency and severity of cyber risks, which are addressed in the following section.

II.1.3 Structural and Technical Factors Driving Cyber Threats

The expansion of global internet connectivity has shifted social and commercial activity online, facilitating the migration of traditional offenses to digital environments.[45] Exploiting digital infrastructure requires specialized technical capacities—such as operating system exploitation, rapid scripting, and vulnerability identification—deployed by individuals, state-backed entities, and organized actors.[46] From a legal governance perspective, these technical vulnerabilities are significant because they represent the specific risk vectors that primary Cybersecurity legislation seek to regulate before they occur..

First, software vulnerabilities stemming from accelerated production, secure coding gaps, and unpatched third-party or cloud dependencies. They permit unauthorized command execution and data exfiltration.[47] Furthermore, software that relies on external services, cloud infrastructure, or third-party integrations can introduce additional risks if these dependencies are misconfigured, outdated, or no longer maintained.[48] In contemporary cybersecurity regulation, certain software vulnerabilities have become the subject of explicit legal obligations concerning secure development, vulnerability handling, supply-chain risk, and, in some regulatory regimes, product conformity.

Second, hardware vulnerabilities hidden within physical components present distinct regulatory challenges, as traditional software security tools cannot easily detect counterfeit or

[45] CHNG et al., 2022, p.2.
[46] ASLAN et al., 2023, p.10.
[47] ASLAN, 2016, p.641.
[48] BUCHMANN – HARTMANN, 2020, p.48.

altered integrated circuits. Hardware security thus creates a need for market-surveillance mechanisms, customs controls, and statutory certification schemes to guarantee the physical integrity of digital products entering the market.

Third, network vulnerabilities arising from legacy protocols (e.g., TCP/IP, DNS) and unsegmented architectures allow malicious actors to intercept or reroute data flows through techniques such as DNS tunneling.[49] Legally, these network weaknesses define the baseline for mandatory "appropriate technical and organizational measures" imposed on essential service operators, establishing the legal standard against which administrative negligence and supervisory sanctions are assessed.

Finally, human and organizational vulnerabilities constitute a critical risk vector. Attackers exploit cognitive factors, such as trust or carelessness, through social engineering and phishing to bypass technical controls.[50] These vulnerabilities justify statutory mandates for mandatory corporate cybersecurity awareness programs, administrative access controls, and strict internal governance duties for corporate management.

The persistent and evolving nature of these technological, network, software, and human vulnerabilities demonstrates that cybersecurity cannot be regulated solely through technical controls or reactive criminal enforcement. Each risk vector creates a corresponding need for legal rules capable of establishing preventive obligations, assigning institutional responsibilities, and ensuring effective incident response.

The conceptual and structural foundations established above therefore provide the basis for examining how legal systems have progressively responded to these risks. The following section traces the historical development of cybersecurity legislation in the EU and Jordan, identifying the principal legal and institutional developments that have shaped their contemporary cybersecurity governance frameworks.

[49] SINGH, 2022, p.309.
[50] ALSHARIF et al., 2022, p.1155.

II.2 Historical Legislative Foundations of Cybersecurity in the EU and Jordan

II.2.1. The development of Cybersecurity Legislation in the EU

As cyber threats have intensified globally, ensuring cybersecurity has become a central strategic objective within the EU. Historically, the lack of adequate protection across networks and digital products was linked to both regulatory fragmentation among Member States and market failures regarding product security standards.[51] The EU progressively developed an integrated, multi-layered legislative strategy designed to establish comprehensive legal governance over its digital ecosystem.

The EU's legislative engagement with cybersecurity governance began in 2004 with the adoption of Regulation (EC) No 460/2004, which established ENISA.[52] While its initial mandate was primarily advisory and focused on technical expertise, the agency provided crucial support to Member States and fostered cross-border institutional cooperation. This marked the foundational step toward a coordinated EU cybersecurity governance regime, laying the structural groundwork for the Union's subsequent binding legislation in this field.

Building on this foundation, the NIS Directive was adopted in 2016 and became legally binding in May 2018, representing the EU's first comprehensive horizontal legislative instrument on cybersecurity,[53] the Directive mandated Member States to adopt national cybersecurity strategies, designate competent national governance authorities, and impose mandatory risk management and incident reporting duties on operators of essential services across critical sectors—such as energy, banking, healthcare, and digital infrastructure.[54] Its primary governance objective was to establish a common baseline level of cybersecurity resilience across the Union.

In parallel, the GDPR also became applicable in May 2018. Although primarily a data-protection instrument rather than a general cybersecurity statute, the GDPR incorporates important security obligations into the governance of personal data.[55] Through statutory principles such as

---

[51] CHIARA, 2022, p.255.
[52] European Parliament and Council of Europe, Regulation No. 460/2004 for the European Network and Information Security Agency.
[53]. European Parliament and Council of the European Union, Directive No. 2016/1148 on the Security of Network and Information Systems Across the Union (NIS Directive).
[54] Ibid.
[55] European Parliament and Council of the European Union, Regulation No. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

data protection by design and by default, mandatory breach notification, and data minimization, it embedded cybersecurity obligations directly into corporate and institutional governance architectures.

To further consolidate this institutional framework, the EU adopted the CSA in 2019.[56] This act enhanced ENISA's institutional role by granting it a permanent mandate equipped with expanded resources and regulatory authority. Crucially, the CSA also introduced the first EU-wide cybersecurity certification framework, aiming to harmonize security standards and assurance levels for digital products, services, and processes across the internal market.

Recognizing the shortcomings of the original NIS Directive, the EU introduced the NIS2 Directive, which entered into force in 2023.[57] This major reform broadened statutory sectoral coverage, strengthened administrative enforcement powers, and promoted greater supervisory harmonization across Member States. Nevertheless, gaps in securing the broader supply chain for digital products persisted, necessitating further horizontal legislative intervention.

In response, the EU enacted the CRA, which entered into force in December 2024. Unlike the voluntary certification framework established under the CSA, the CRA created mandatory, horizontal cybersecurity requirements for all products with digital elements placed on the EU market. By enforcing legal duties for security-by-design, transparent vulnerability handling, and mandatory ongoing security updates throughout the product lifecycle, the CRA addressed long-standing regulatory gaps left by earlier legislation.[58]

Most recently, the EU enacted the Cyber Solidarity Act, effective from 4 February 2025 to bolster its collective capacity to detect, prepare for, and respond to significant and large-scale cyber incidents.[59] The Act established a European Cybersecurity Alert System based on a pan-European network of National Cyber Hubs and Cross-Border Cyber Hub.[60] Additionally, it facilitates the

[56] European Parliament and Council of the European Union, Cybersecurity Act No. 2019/881.
[57] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive).
[58] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act).
[59] European Parliament and Council of the European Union, Regulation (EU) 2025/38 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act).
[60] GTG Legal, The EU's next step in resilience: the Cyber Solidarity Act and amendments to the Cybersecurity Act, https://www.gtg.com.mt/cyber-solidarity-act-eu-cybersecurity-legislation/. (Accessed 18 October 2025).

creation of a European Cybersecurity Reserve, drawing upon trusted private sector providers to support emergency responses.[61]

II.2.2 Roots of Cybersecurity Legislation in Jordan

Jordan, as an emerging jurisdiction, has been actively working to modernize its cybersecurity legal system, driven in part by the absence of unified regional standards for cybersecurity and data protection in the Middle East. In this context, the Kingdom has progressively introduced national statutes and regulatory instruments to mitigate evolving digital risks and protect national critical infrastructure.

Following the enactment of Jordanian Cybersecurity Law in 2019,[62] several executive regulations and administrative instructions were issued to operationalize its statutory framework. For instance, Regulation No. 1 of 2020 on the NCSC established a comprehensive licensing and oversight strategy for cybersecurity service providers, including managed security, incident response, penetration testing, and digital forensics.[63] This regulatory framework aimed to ensure service quality, technical accountability, and institutional integrity while fostering trust between service providers and client institutions, ultimately strengthening the overall resilience of Jordan's digital ecosystem.

In line with these governance objectives, Regulation No. 25 of 2021 further refined the organizational and operational structure of the NCSC, detailing its executive leadership, specialized directorates, and operational units.[64] The regulation clarified the Center's statutory roles and responsibilities, empowering it to manage national cybersecurity strategies, coordinate multi-sectoral incident responses, and maintain centralized operational oversight across public and private infrastructure.[65]

Complementing these institutional efforts, the Instructions for the Classification of Cybersecurity Incidents were issued in 2023, establishing a standardized framework for categorizing cybersecurity incidents into four distinct severity levels: Severe, Serious, Medium,

---

[61] European Parliament and Council of the European Union, Regulation (EU) 2025/38 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act), Articles (1,2,3).
[62] Jordan, Cybersecurity Law No. 16 of 2019.
[63] Jordan, National Cybersecurity Center Regulation No. 1 of 2020.
[64] Jordan, Jordan, Administrative Organization Regulation of the National Cybersecurity Center No. 25 of 2021.
[65] Ibid., Article 5(C).

and Low.[66] This classification scheme ensured consistent risk assessment, standardized prioritization, and uniform incident response procedures across regulated entities, thereby promoting operational clarity within domestic governance protocols.

In parallel, the PDPL No. 24 of 2023, which became effective in March 2024, established Jordan's first standalone statutory framework for personal data governance.[67] It introduced explicit legal obligations regarding lawful data processing, secure storage, and mandatory breach reporting, thereby reinforcing national cybersecurity governance measures and promoting trust in digital governance systems.

Following these statutory developments, the Regulation for the Licensing of Cybersecurity Service Providers for 2024 established a formal regulatory licensing scheme, requiring commercial service providers to obtain formal authorization from the NCSC.[68] The regulation aims to ensure that cybersecurity services, such as risk assessments, monitoring, incident response, and consulting, are delivered by qualified and accountable entities in accordance with national security priorities and international best practices.

Finally, the Instructions for Determining the Criteria of Violations of the Cybersecurity Law and Their Procedures for 2025 delineated specific administrative enforcement mechanisms and penalties for non-compliance, such as failure to notify the NCSC of security incidents or failure to implement mandated technical mitigation controls.[69] Collectively, these developments demonstrate the progressive expansion of Jordan's cybersecurity legal and institutional framework from a primarily criminal-law-oriented approach toward a broader system incorporating institutional coordination, incident management, service-provider regulation, data protection, and administrative enforcement.

---

[66] Jordan, Instructions for the Classification of Cybersecurity Incidents for the Year 2023, issued pursuant to Clause (3) of Paragraph (b) of Article 6 of the Cybersecurity Law No. 16 of 2019, 2023, available at: https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/cyber_security_incidents_categorization_instructions_2023.pdf, (Accessed on 21 October 2025).
[67] Jordan, PDPL No. 24 of 2023.
[68] Jordan, Cybersecurity Service Providers Licensing Regulation No. 76 of 2024.
[69] Jordan, Instructions for Determining the Criteria for Violations of the Provisions of the Cybersecurity Law, Their Controls and the Procedures Due Thereto for the Year 2025.

II.3 Chapter Conclusion

This chapter has established the conceptual and historical foundations for examining cybersecurity as a distinct field of legal governance. The conceptual analysis demonstrated that cybercrime represents only one dimension of harmful digital activity, while cyber threats and cybersecurity incidents also encompass technical failures, vulnerabilities, human error, and other disruptions requiring preventive and administrative responses. The analysis of structural and technical vulnerabilities further showed that cybersecurity cannot be secured through criminal sanctions alone, but requires legal mechanisms addressing prevention, risk management, and incident response.

The historical analysis demonstrated that both the EU and Jordan have progressively developed legislative and institutional frameworks in response to these challenges, although through different institutional and regulatory trajectories. The EU has evolved toward an integrated framework combining risk management, incident reporting, data protection, product security, and cyber resilience, while Jordan has progressively expanded its framework through the Cybersecurity Law, NCSC regulations and instructions, and the PDPL.

Accordingly, this chapter provides the criteria for assessing the substantive effectiveness of contemporary cybersecurity frameworks. The following chapters build on this foundation by examining the EU and Jordanian legal frameworks in detail, focusing on their regulatory mechanisms, institutional structures, preventive and responsive obligations, and overall capacity to provide coherent cybersecurity governance.

Chapter III: The EU Legal and Regulatory Framework for Cybersecurity

III.1 Core Cybersecurity Legislation

III.1.1 The NIS Directive

The EU has been steadily advancing and reinforcing its cybersecurity governance framework since 2004, beginning with the establishment of ENISA.[70] This institutional foundation signaled the Union's recognition of cybersecurity as a key pillar of digital trust, resilience, and strategic autonomy. While the introductory provisions of the Directive established the necessary

[70] European Parliament and Council of Europe, Regulation No. 460/2004 for the European Network and Information Security Agency.

administrative governance and coordination mechanisms, its deeper significance lies in how it operationalized cybersecurity risk management across critical sectors and elevated the issue to a matter of collective European concern.[71]

The primary objective of the NIS Directive was to strengthen the overall cybersecurity posture and systemic resilience of the Union by obliging Member States to adopt a national strategy for securing network and information systems and to designate competent national governance authorities responsible for its implementation and oversight.[72]

In addition, the directive introduced concrete statutory obligations for operators of essential services and digital service providers, particularly within critical sectors such as energy, transport, banking, healthcare, and digital infrastructure.[73] These obligations included the adoption of preventive (*ex-ante*) risk management practices,[74] the implementation of appropriate technical and organizational measures,[75] mandatory incident reporting of significant cybersecurity incidents to national authorities,[76] and establishing Computer Security Incident Response Teams (CSIRTs).[77]

III.1.1.1 Operators of Essential Services

Operators of essential services constitute the first category of entities within the scope of the NIS Directive. An operator of essential services is defined as a public or private entity that operates in specific sectors, such as the sector of energy, transport, banking and health, and which at the same time meets some essential criteria that qualify it as an entity of such type.[78] Those operators of essential services must adopt appropriate technical and organizational measures to manage risks affecting the security of their network and information systems. These measures must aim to prevent and minimize the impact of incidents, ensuring the continuity of essential societal services.

While the Directive sets out a harmonized obligation at EU level, the detailed implementation of security requirements remains largely within the discretion of Member States. To promote alignment and consistency, the European Commission and the NIS Cooperation Group

[71] WEBBER – TAYLOR, 2016, p.9.
[72] European Parliament and Council of the European Union, Directive No. 2016/1148 on the Security of Network and Information Systems Across the Union (NIS Directive). Articles (1,7,8).
[73] Ibid., Article 4(4), Annex II.
[74] Ibid., Article 14.
[75] Ibid., Articles (14,16).
[76] Ibid.
[77] Ibid., Articles (9,11).
[78] Ibid., Articles (4(4), 5(1,2)).

have issued guidance recommending that national measures be effective, proportionate, verifiable, and tailored to sector-specific risks.

In addition to preventive obligations, operators of essential services must notify their competent national authorities or CSIRTs of any incidents that significantly impact the continuity of the services they provide. The Directive establishes qualitative criteria to assess the significance of such incidents, including the number of users affected, the duration of disruption, and the geographical extent of the impact. Minor or routine technical events fall outside the notification requirement.[79] Crucially, from a legal governance perspective, this restrictive threshold risks excluding security breaches that compromise the confidentiality, integrity, or authenticity of data without immediately disrupting service continuity, thereby limiting the Directive's preventive and resilience-building potential.

For instance, in September 2018, prior to the United Kingdom's withdrawal from the EU, British Airways experienced a major data breach that exposed the personal and financial details of approximately 380,000 customers after attackers gained access to the company's servers and altered its website code. Despite the seriousness of the breach, it did not cause flight delays or cancellations, and thus fell outside the primary availability-focused incident reporting thresholds of the original NIS framework, illustrating how critical cybersecurity vulnerabilities may fall outside traditional continuity-focused reporting frameworks.[80]

A further limitation lies in the uneven institutional capacity of national and sectoral authorities to implement and enforce the Directive's obligations consistently across the EU. The NIS framework presupposes that competent administrative authorities possess the technical expertise necessary to assess cybersecurity risks, interpret incident reports, and evaluate compliance by operators of essential services. In practice, however, many regulators particularly those originating from safety or reliability focused domains lacked prior experience in managing cyber threats and had to build such expertise from the ground up.[81]

This institutional gap was mirrored on the operational side, the Directive's reliance on broad, principle-based obligations, requiring "appropriate and proportionate" measures created

[79] Ibid., Article 14(3,4,5).
[80] MICHELS – WALDEN, 2020, p.36.
[81] Ibid., p.35.

legal uncertainty for operators of essential services, who were left to interpret what compliance entailed.[82] Practically, many organizations adopted common cybersecurity capabilities to meet these requirements. To provide greater legal clarity, some Member States, such as Belgium, explicitly recognized ISO/IEC 27001 certification as presumptive evidence of compliance, translating the Directive's abstract duties into concrete technical standards.[83]

In addition to these substantive and institutional challenges, the NIS Directive also faced jurisdictional limitations stemming from divergent national interpretations of key legal concepts such as "establishment." This inconsistency often resulted in fragmented oversight of cross-border operators of essential services, complicating compliance and enforcement efforts across the EU.[84]

III.1.1.2 Digital service providers

Digital service providers are the second category of entities that fall under the scope of the NIS Directive. Digital service providers include any legal person that provides a digital service,[85] and more specifically an online market place, an online search engine, or a cloud computing service.[86] However, while this definition usefully establishes clear service categories, it does not fully reflect the complexity of the digital economy and creates interpretative ambiguity regarding which online activities qualify as "digital services".

These entities are regulated because of their systemic importance to other sectors and their potential to cause widespread disruption in the digital economy.[87] Unlike operators of essential services, Member States are not required to identify individual digital service providers, reflecting a "catch-all" approach that automatically brings such entities within the Directive's scope.[88] Their inclusion recognizes that disruptions to digital platforms could undermine economic activity and public trust across the internal market.

---

[82] Deloitte Belgium, Developing cybersecurity capabilities for EU NIS Directive, available at: https://www.deloitte.com/be/en/services/consulting-risk/research/developing-cybersecurity-capabilities-for-eu-nis-directive.html (Accessed 5 November 2025). See also European Parliament and Council of the European Union, Directive No. 2016/1148 on the Security of Network and Information Systems Across the Union (NIS Directive). Article 14(1).
[83] Belgium: Act of 7 April 2019 on the Security of Network and Information Systems, Article 22(1).
[84] Contreras, 2023, p.330.
[85] European Parliament and Council of the European Union, Directive No. 2016/1148 on the Security of Network and Information Systems Across the Union (NIS Directive). Article 4(6).
[86] Ibid., Article 4(17,18,19).
[87] Ibid., Recital 48.
[88] Ibid., Article 16(1).

Digital service providers must implement proportionate risk management measures safeguard their network and information systems, focusing on system integrity, incident handling, business continuity, monitoring, and compliance with international standards.[89] For instance, they are required to notify incidents with a "substantial impact" on their services, evaluated through factors such as user numbers, disruption duration, geographical spread, and economic or societal effects.[90] However, their regulatory regime is lighter than that of essential service operators: competent authorities act mainly through reactive (*ex-post*) supervision, and notification duties apply only when the provider possesses sufficient information to assess an incident's impact.[91]

To ensure legal and operational consistency, the European Commission adopted Implementing Regulation (EU) 2018/151, which provides detailed specifications on the security measures and incident notification parameters applicable to digital service providers.[92] This implementing act establishes a harmonized and consistent baseline for compliance across all Member States, thereby promoting the uniform application of the NIS Directive's provisions throughout the Union.

However, despite its objective of ensuring uniformity, Implementing Regulation (EU) 2018/151 has faced criticism for adopting an overly rigid and standardized approach that may not reflect the varying risk environments of digital service providers. The use of fixed quantitative thresholds to assess the "substantial impact" of incidents limits regulatory flexibility and may fail to capture the subtle complexity of modern supply-chain cyber risks. In addition, the Regulation provides limited guidance on qualitative factors, such as reputational harm or third-party service disruption, resulting in uneven interpretation among Member States.

III.1.2 Cybersecurity Act (CSA)

The EU CSA represents a significant advancement in the EU's cybersecurity legal architecture. It builds upon earlier legislative efforts by establishing a comprehensive and enduring approach to enhancing cybersecurity across the Union.[93] The Act grants ENISA a permanent mandate,

[89] Ibid., Article 16(2).
[90] Ibid., Article 16(3,4), Recital 57.
[91] Ibid., Article 17(1), Recital 65.
[92] European Commission, Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for the application of Directive (EU) 2016/1148 as regards further specification of the elements to be taken into account by digital service providers and parameters for determining substantial incident impact.
[93] European Parliament and Council of the European Union, Cybersecurity Act No. 2019/881. Articles (1,3), Recital 1.

expanding its financial and human resources and strengthening its strategic role in supporting the EU's objective of achieving a common, high level of cybersecurity.[94] Through this reform, ENISA's functions extend beyond advisory and coordination tasks to include the operational support of Member States and EU institutions in responding to cybersecurity incidents and policy development.[95]

A key innovation introduced by the Act is the establishment of the first EU-wide cybersecurity certification framework.[96] This framework aims to create a harmonized and trusted system for certifying ICT products, services, and processes, thereby reducing market fragmentation and improving the overall resilience of the internal digital market.[97] Under this Act, ENISA is tasked with developing European cybersecurity certification schemes, such as the European Union Common Criteria (EUCC) scheme, and aligned with broader horizontal European and international standards.[98]

Certification under this model is voluntary and risk-based, allowing self-assessment for low-risk products while defining three assurance levels-basic, substantial, and high-to reflect differing levels of security assurance, costs, and practical needs.[99] Despite the voluntary certification nature of under CSA, the act expressly permit exceptions under Union or national law and empower the EU legislature to introduce mandatory certification schemes where heightened cybersecurity risks dictate.[100] Indeed, the certification framework contributes to increasing trust in digital products and promoting standardization across Member States by fostering interoperability and mutual recognition among national certification bodies.[101]

Building on this foundation, the implementation of essential cybersecurity requirements under EU harmonization legislation further underscores the importance of developing coherent and cross-sectoral standards to guide compliance. Horizontal security standards which establish

[94] Ibid., Article 1(1)(a).
[95] Ibid., Articles 3(1,2), 7(1)(d), 10(1).
[96] Ibid., Article 46.
[97] Ibid., Article 46(1), Recitals (65, 66, 67).
[98] Ibid., Articles (49,50). See also European Union Agency for Cybersecurity, EU Cybersecurity Certification Scheme on Common Criteria, 2024, available at: https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en (Accessed 9 June 2026).
[99] European Parliament and Council of the European Union, Cybersecurity Act No. 2019/881. Article 52.
[100] Ibid., Article 56(2,3).
[101] KHURSHID et al., 2022, p.129935.

fundamental security principles applicable to a broad range of products and systems are central to this effort.

Standards series such as the EN ISO/IEC 27000,[102] and EN IEC 62443,[103] are particularly well-suited to fulfil the security objectives of multiple EU instruments. Their adoption not only enhances the security and reliability of connected products but also contributes to reducing regulatory overlap and fragmentation, thereby reinforcing coherence and trust across the European digital ecosystem.[104]

However, despite these advantages, the framework has faced several legal and practical criticisms. The voluntary nature of certification leaves manufacturers under no legal obligation to certify ICT products, limiting the scheme's capacity to ensure a consistent baseline of cybersecurity across the Union. Furthermore, the EUCC scheme, which is the only fully developed certification model to date, focuses primarily on general ICT products and lacks sufficient granularity to address sector-specific challenges or rapidly evolving technologies such as IoT devices.

From a legal governance perspective, the CSA represents a crucial step toward the consolidation of cybersecurity governance within the EU by combining institutional empowerment with market-oriented regulatory mechanisms. Nonetheless, its reliance on voluntary participation and the absence of mandatory enforcement provisions reveal an inherent tension between regulatory flexibility and legal certainty. This structural limitation, while fostering innovation and industry engagement, may also undermine the Act's preventive and harmonizing potential, particularly in high-risk domains that demand stronger regulatory oversight.

This critique is further substantiated by recent academic evaluations of the CSA's implementation, particularly regarding the minimum-security objectives outlined in Article 51. Recent analytical evaluations reveal notable interpretative and practical limitations, finding significant variation in how these objectives are understood, alongside structural gaps, such as

[102] International Organization for Standardization (ISO), ISO/IEC 27001 — Information Security Management, available at: https://www.iso.org/isoiec-27001-information-security.html (Accessed 7 November 2025).
[103] International Electrotechnical Commission, Cybersecurity — Official IEC Cybersecurity Portal, available at: https://www.iec.ch/cybersecurity/?ref=extfooter (Accessed 7 November 2025).
[104] KOHLER, 2020, p.11.

incomplete rules on restorability, vulnerabilities in secure updates, and limited lifecycle applicability.[105]

III.1.3 NIS2 Directive

The steady escalation of cybersecurity incidents across the EU had revealed significant weaknesses in the existing regulatory framework and underscored the necessity for legislative reform, particularly regarding the NIS Directive.[106] According to Eurostat, approximately 22% of EU enterprises had experienced ICT-related security incidents in 2021, compared to only 12% in 2018, [107] reflecting a substantial rise in digital vulnerabilities across the internal market. Other study revealed that ransomware attacks were growing by 41% and email-based threats, including phishing, increasing by 48% in 2022.[108]

In response to these deficiencies, the European Commission proposed the NIS2 Directive on 16 December 2020, initiating the legislative process aimed at establishing a high, common level of cybersecurity across the Union. Following approximately 18 months of negotiations, the proposal was endorsed by the Industry, Research and Energy Committee on 13 July 2022 and subsequently approved by the European Parliament on 10 November 2022.[109]

The Directive was formally adopted on 14 December 2022 and published in the Official Journal of the European Union as Directive (EU) 2022/2555. It entered into force on 16 January 2023, and Member States were given 21 months—until 17 October 2024—to adopt and publish the national measures necessary for its transposition.[110]

NIS2 Directive significantly expanded both the sectoral scope and regulatory reach of EU NIS Directive, extending coverage to new domains such as postal and courier services,[111] while setting clear thresholds to include all medium and large entities in critical sectors. [112] Member

[105] FERGUSON, 2022, p.104.
[106] VANDEZANDE, 2024, p.1.
[107] Eurostat, 22% of EU Enterprises Had ICT Security Incidents, 14 February 2023, available at: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20230214-1 (Accessed 11 November 2025).
[108] Security Staff, Email Cyberattacks Increased 48% in First Half of 2022, Security Magazine, 11 August 2022, available at: https://www.securitymagazine.com/articles/98145-email-cyberattacks-increased-48-in-first-half-of-2022 (Accessed 11 November 2023).
[109] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive).
[110] Ibid., Articles (40,41).
[111] Ibid., Article 2(1). Annex (I, II).
[112] Ibid., Article 2(1,2).

States retained discretion to designate smaller, high-risk entities, maintaining proportionality and flexibility in implementation.[113]

This broadened approach reflected a structural recalibration of how cybersecurity responsibilities are allocated across the Union. NIS2 established a more comprehensive framework for identifying entities within its remit, ensuring that administrative oversight extended to critical sectors underpinning Europe's digital and economic resilience.

In terms of its detailed scope, the Directive applied to medium-sized and larger public or private entities operating in highly critical sectors listed in Annex I,[114] as well as other critical sectors enumerated in Annex II.[115] This expansion covered electricity generation, district heating, hydrogen infrastructure, healthcare, water management, digital infrastructure, cloud services, content delivery networks, ICT service management, manufacturing of medical devices, and research organizations.

While small and micro-enterprises (SMEs) were generally exempted,[116] entities of any size could be included if they provided public electronic communications networks, top-level domain name services, or essential functions whose disruption could trigger systemic cross-border risks.[117] The Directive further extended coverage to trust service providers, which were previously partially exempt under NIS1,[118] and to central and regional public administrations, recognizing the criticality of government digital services.[119] This represented a major departure from NIS1, which had granted Member States wide discretion in identifying operators of essential services, resulting in fragmented national implementations.[120]

The Directive distinguished between essential and important entities, defining essential entities as those fundamental to their sectors, critical for societal or economic activities, or

[113] Ibid., Articles (2(2), 3).
[114] Ibid., Annex 1.
[115] Ibid., Annex 2.
[116] Ibid. Article 2(1).
[117] Ibid., Article 2(2).
[118] Ibid., Article 2(2)(a)(ii), Recital 9.
[119] Ibid., Article 2(2)(f), Annex I (8).
[120] European Parliament and Council of the European Union, Directive No. 2016/1148 on the Security of Network and Information Systems Across the Union (NIS Directive). Article 5(1,2).

uniquely providing indispensable services within member state.[121] Important entities encompassed all other actors within Annexes I and II not meeting the essential criteria.[122]

Notwithstanding this attempt at statutory clarity, legal scholars such as Chałubińska-Jentkiewicz and Nowikowska have critiqued this binary classification for its conceptual inconsistencies, arguing that the distinction conflates an entity's size with its inherent sector criticality.[123]

For instance, an entity of similar size and societal relevance operating in an Annex II sector (e.g. manufacturing or food supply) is deemed only an 'important entity,' while one in an Annex I sector (e.g. energy) is classified as 'essential,' even if their potential systemic impact is comparable. This illustrates how the binary categorization may not fully align with actual risk exposure.[124]

This broadened coverage was estimated to affect over 160,000 entities across the EU, reflecting the growing pervasiveness of cyber threats and the need for a harmonized cybersecurity framework across diverse sectors.[125] NIS2 maintained minimum harmonization principles, allowing coexistence with sector-specific regimes where equivalent cybersecurity requirements applied, while establishing itself as the core legislative framework of EU cybersecurity governance.[126]

Beyond redefining statutory scope, NIS2 introduced a robust administrative framework for cybersecurity governance. It strengthened risk management and incident reporting obligations by establishing harmonized minimum-security requirements and standardized reporting timelines.[127] Crucially, it adopted an *ex-ante* risk-based approach, requiring entities to identify and mitigate cybersecurity risks across their operations, software supply chains, and third-party service

[121] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 3(1).
[122] Ibid., Article 3(2), Recital 21.
[123] CHAŁUBIŃSKA – NOWIKOWSKA, 2024, p.7.
[124] Ibid.
[125] VANDEZANDE, 2024, p.6.
[126] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Articles (4,5).
[127] Ibid., Articles (21, 23(1,2,3,4,5)).

providers.[128] By embedding supply-chain accountability into primary legislation, NIS2 moved beyond mere organizational compliance to establish a regime of statutory collective responsibility.

The Directive reinforces oversight through stricter supervisory and enforcement mechanisms. It introduces more intrusive supervisory powers for competent authorities and harmonized minimum penalties across the Union.[129] Essential entities may face fines of at least €10 million or 2% of global annual turnover,[130] while important entities may be sanctioned up to €7 million or 1.4% of turnover,[131] alongside non-monetary penalties such as compliance orders or public reprimands.[132] This alignment aims to ensure a consistent sanctions regime across Member States and to enhance regulatory deterrence.[133]

NIS2 further seeks to promote coherence across the EU's cybersecurity framework by aligning its risk-management requirements with related legislative instruments, most notably the CER Directive,[134] thereby avoiding duplication of obligations and ensuring a coordinated approach to the protection of critical and essential services.[135]

Building on its effort to harmonize EU cybersecurity legislation, NIS2 also complements the CSA by promoting the use of European cybersecurity certification schemes for ICT products, services, and processes.[136] According to the directive, Member States may require essential and important entities to adopt certified solutions to demonstrate compliance with NIS2 risk-management obligations, while the Commission can specify which entities must use particular certified products or obtain certificates where cybersecurity levels are deemed insufficient.

However, if no appropriate European certification scheme exists, ENISA may develop a candidate scheme, ensuring a consistent and harmonized approach across the Union, reducing

[128] Ibid., Article 21(1,2).
[129] Ibid., Articles (32,33,34).
[130] Ibid., Article 34(4).
[131] Ibid., Article 35(5).
[132] Ibid., Articles (32(4,5), 33(4).
[133] GAIE – MUECK, 2025, p.176
[134] European Parliament and Council of the European Union, Directive (EU) 2022/2557 of 14 December 2022 on the Resilience of Critical Entities.
[135]European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 4, Recitals (7, 96).
[136] Ibid., Article 24.

duplicative national certifications, lowering implementation costs, and strengthening overall cybersecurity resilience.[137]

Despite advantages of NIS2, the implementation has introduced new challenges. A primary concern relates to the financial and operational burden imposed on regulated entities. The European Commission estimated an average increase in ICT expenditure of approximately 0.63% of total turnover for organizations newly brought within the Directive's scope, and 0.58% for those already covered under NIS1.[138] These additional compliance costs were expected to cascade through the digital value chain, potentially influencing the final cost of digital goods and services.

This financial burden is particularly acute for certain small entities that fall under the Directive's scope regardless of their size. As noted by scholars, Article 2(2) of NIS2 brings specific "sensitive" entities, such as top-level domain registries, DNS providers, and trust service providers into the regulatory fold purely based on their critical function, with no size-based exemption. This creates a situation where these often-smaller organizations face the full weight of compliance, requiring specialized and potentially costly services to meet the same standards as large corporations.[139]

Despite its more comprehensive design, the NIS2 framework did not entirely eliminate the fragmentation that had characterized the EU's cybersecurity landscape. Because directives required transposition into national law, variations persisted in how Member States interpreted and implemented key provisions, leading to differences in enforcement intensity and compliance expectations. This uneven transposition risked perpetuating regulatory disparities and undermining the goal of a fully harmonized cybersecurity regime within the internal market.[140]

Overall, the NIS2 Directive represented a substantial evolution in the EU's cybersecurity governance model. By extending its scope, strengthening supply chain oversight, and imposing harmonized risk management duties, it established a more resilient and future-oriented framework.

---

[137] Ibid., Article 24(3).
[138] European Commission, Impact Assessment Report Accompanying the Proposal for a Directive on Measures for a High Common Level of Cybersecurity Across the Union, SWD (2020) 345 final, Part 1, p.74.
[139] PORZEŻYŃSKI – KULICKI, 2024, p.33.
[140] Kosciuszko Institute and European Cyber Security Organization, Eliminating Difficulties and Challenges in Implementing Legislative Solutions in the Area of Cybersecurity – DORA, NIS2: Second Policy Brief (2024), available at: https://ik.org.pl/wp-content/uploads/2025/01/Eliminating-difficulties-and-challenges-in-implementing-legislative-solutions-in-the-area-of-cybersecurity-%E2%80%93-DORA-NIS2.pdf (Accessed 30 October 2025).

Yet, its effectiveness ultimately depended on consistent national implementation and on the EU's ability to ensure that NIS2 operated in concert with parallel legal instruments such as CSA and CRA to deliver a coherent and robust cybersecurity architecture across the Union.

III.1.4 Cyber Resilience Act (CRA)

Cyber resilience refers to the capacity of digital systems and organizations to anticipate, withstand, recover from, and adapt to cyber incidents, relying on a combination of technical safeguards, organizational policies, and human governance.[141] This concept has gained increasing relevance as digital products including software, hardware, and hybrid systems, have become deeply embedded in critical societal and economic functions.

The EU's CRA responds to long-standing market failures in securing digital products and represents the first EU-wide attempt to impose horizontal, mandatory cybersecurity requirements across all products with digital elements.[142] The Act aims to strengthen the cybersecurity of digital products throughout their entire lifecycle,[143] addressing challenges that voluntary schemes under earlier frameworks, including the EU CSA, could not sufficiently resolve.

The CRA was initiated by the European Commission, building on the EU's 2020 Cybersecurity Strategy for the Digital Decade.[144] As stated by the EU Commission's President von der Leyen, "If everything is connected, everything can be hacked … This is why we need … legislation on common standards under a new European Cyber Resilience Act".[145] This framing positions the CRA as a legislative response to the strategic objectives set out in 2020, aiming to create a unified and mandatory framework for securing products with digital elements across the EU.

The act is also designed to address significant regulatory gaps left by the CSA's voluntary certification framework for digital products, thereby strengthening the EU's institutional

[141] KOTT – LINKOV, 2019, p.176.
[142] BURRI – ZIHLMANN, 2023, p.B13.
[143] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), Article 13.
[144] European Commission, The EU's Cybersecurity Strategy in the Digital Decade, 16 December 2020, available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade (Accessed 16 November 2025).
[145] European Commission, How a European Cyber Resilience Act Will Help Protect Europe, 16 September 2021, available at: https://commissioners.ec.europa.eu/how-european-cyber-resilience-act-will-help-protect-europe-2021-09-16_en (Accessed 16 November 2025).

cybersecurity posture.[146] This gap has been clearly revealed when manufacturers largely avoided adopting these voluntary standards due to cost considerations and the absence of legal incentives.[147]

This limited the CSA's ability to mitigate systemic vulnerabilities, particularly within the rapidly expanding ecosystem of interconnected digital products. Recognizing that voluntary certification was insufficient to address widespread weaknesses, especially in low-cost digital devices that frequently lacked even basic security safeguards, the EU subsequently introduced mandatory cybersecurity requirements.

To this extent, the proposal of the act was first announced in 2021, formally proposed by the Commission on 15 September 2022, and then progressed rapidly through the institutional process.[148] A political agreement between the European Parliament and the Council was reached on 1 December 2023,[149] paving the way for final adoption. Following publication in the Official Journal of the European Union in 20 November 2024, the CRA entered into force 20 days after publication, thereby triggering its implementation timeline.[150]

Following its publication in the Official Journal of the European Union on 20 November 2024, the CRA entered into force on 10 December 2024, thereby triggering its phased implementation timeline. Rather than imposing immediate compliance, the regulation provides economic operators and Member States with a general 36-month transitional application period—until 11 December 2027—to achieve full product conformity with its essential cybersecurity

[146] European Commission, Commission welcomes political agreement on Cyber Resilience Act, Press Corner, 1 December 2023, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6168 (Accessed 16 November 2025). See also CRA's recitals (3,4).
[147] European Commission, Impact Assessment Report Accompanying the Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020, SWD (2022).
[148] European Commission, State of the Union: New EU cybersecurity rules ensure more secure hardware and software products, Press Corner, 15 September 2022, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5374 (Accessed 16 November 2025).
[149] Council of the European Union, Cyber Resilience Act: Council and Parliament Strike a Deal on Security Requirements for Digital Products, Press Release, 30 November 2023, available at: https://www.consilium.europa.eu/en/press/press-releases/2023/11/30/cyber-resilience-act-council-and-parliament-strike-a-deal-on-security-requirements-for-digital-products/ (Accessed 16 November 2025).
[150] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), Article 71.

requirements, while manufacturer reporting obligations for actively exploited vulnerabilities and severe incidents take effect earlier, at 21 months.

A central feature of the CRA is its broad statutory scope, applying to any software or hardware product and its remote data processing solutions, including components marketed separately.[151] This formulation definitively brings standalone software within its ambit, addressing past uncertainty over whether the law applied only to physical devices or to software provided independently.[152]

At the same time, the CRA maintains targeted exclusions under certain conditions for sectors already regulated under specialized technical regimes such as medical devices,[153] automotive,[154] aviation systems,[155] and products designed for national security or military use.[156] This reflects an effort to avoid duplicating existing legislative requirements.

Similarly, Software as a Service is excluded due to its service-based operational model, which raises considerations distinct from those of digital products.[157] These boundaries demonstrate a balancing act: expanding regulatory oversight while maintaining coherence with pre-existing sectoral legislation and preserving space for innovation.

The substantive requirements of the CRA fall within several interlinked domains. Manufacturers must ensure that all products placed on the market meet essential cybersecurity standards,[158] fundamentally embedding security-by-design principles into product development.[159] These include secure default configurations, minimization of attack surfaces,[160] adequate logging capabilities, and resilience against common exploitation techniques.[161]

Importantly, the CRA conceptualizes cybersecurity not as a one-time requirement but as a continuous process; manufacturers must establish and maintain vulnerability handling procedures,

[151] Ibid., Article 2.
[152] CHIARA, 2022, p.258.
[153] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act). Article 2(2) (a,b).
[154] Ibid., Article 2(2) (A, B).
[155] Ibid., Article 2(3).
[156] Ibid., Article 2(7).
[157] Ibid., Article 3, Recitals (11,12).
[158] Ibid., Article 13(1), Annex I, Part I (1).
[159] Ibid., Annex I, Part I (2)(b).
[160] Ibid., Annex I, Part I (2)(j).
[161] Ibid., Article 13, Annex I, Part I (2)(I).

including mechanisms for identifying, patching, disclosing, and reporting vulnerabilities throughout the product lifecycle.[162]

They must also maintain comprehensive technical documentation and respond to cybersecurity incidents in a timely manner.[163] National authorities are empowered to conduct market-surveillance and enforce compliance, with the capacity to withdraw or restrict unsafe products and impose penalties where necessary.[164] These provisions reflect a lifecycle-oriented approach aimed at addressing systemic vulnerabilities that previously persisted due to inconsistent market practices.[165]

To ensure proportionality while maintaining a high level of cybersecurity, the CRA employs a risk-based classification system.[166] Products with digital elements are categorized into different risk tiers, with important products listed in Annex III (further divided into Class I and Class II based on their risk profiles) and critical products designated in Annex IV.[167] Class II and critical products encompass items with greater potential to affect safety, security, or network integrity, thereby subjecting them to the most rigorous conformity assessment processes and stricter regulatory controls due to their essential role in digital infrastructure.

This classification mechanism draws directly from lessons learned under the CSA, which relied on voluntary certification; by contrast, the CRA gives the Commission authority to update product categories and technical specifications in response to emerging threats, ensuring a flexible and dynamic regulatory framework. The integration of mandatory conformity assessment procedures—which scale dynamically from internal control self-assessment to mandatory third-party verification depending on the product's risk classification and adherence to harmonized standards—marks a vital shift from the CSA's voluntary approach, transforming baseline security goals into enforceable legal obligations and thereby strengthening overall cyber resilience.[168]

---

[162] Ibid., Annex I, Part II.
[163] Ibid., Article 31.
[164] Ibid., Articles (52,53,54).
[165] Hein, Tatjana, The Cyber Resilience Act and Its Impact on Security in the IoT, dotMag – Building Trust in the Digital World, May 2024, available at: https://www.dotmagazine.online/issues/building-trust-in-the-digital-world/the-cyber-resilience-act-iot-security (Accessed 17 November 2025).
[166] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act). Articles (7,8).
[167] Ibid., Annex III, Annex IV.
[168] AJMERA, 2025. p.7.

To this extent, it is worth mentioning that, establishing enforceable cybersecurity obligations across digital products by CRA addresses the systemic vulnerabilities and market gaps that voluntary frameworks like the CSA could not resolve. Its lifecycle-oriented approach, supported by risk-based product classification and targeted regulatory flexibility, strengthens the EU's overall digital resilience and fosters trust in interconnected technologies. In doing so, the Act consolidates cybersecurity governance at both national and market levels, creating a coherent and adaptive framework capable of responding to emerging threats.

Despite the advantages, the enactment of the CRA carries significant economic challenges. Manufacturers and importers must now absorb substantial compliance costs associated with implementing security-by-design practices, conducting conformity assessments, maintaining documentation, and fulfilling incident reporting and notification obligations.

Importers must further ensure that only compliant products bearing appropriate CE markings enter the EU market, reinforcing accountability in global supply chains. According to the Commission's impact assessment, aggregated compliance costs across the EU market could reach approximately €29 billion, a figure reflecting activities spanning accreditation, market-surveillance, vulnerability management, and regulatory reporting.[169]

Many non-EU manufacturers, particularly those operating in markets with limited security requirements, will face increased costs to meet EU-level standards—costs that may be passed on to consumers in the form of higher product prices. This mirrors trends observed in other regulatory domains, such as the US Food Safety Modernization Act (FSMA),[170] where strengthened compliance obligations likewise increased operational costs for producers.[171]

SMEs form another dimension of the CRA's economic challenge. Although the Act primarily targets manufacturers and operators of digital products, and particularly large organizations,[172] the obligations imposed by the CRA inevitably cascade through supply chains,

[169] European Commission, Commission Staff Working Document – Executive Summary of the Impact Assessment Report Accompanying the Proposal for a Regulation for the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020, SWD(2022) 283 final, 15 September 2022, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52022SC0283 (Accessed 16 November 2025).
[170] United States, Food Safety Modernization Act, Pub. L. No. 111-353, 124 Stat. 3885 (2011).
[171] ADALJA – LICHTENBERG, 2018, p.33.
[172] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), Articles (13,32,33).

indirectly affecting these enterprises.[173] Many smaller entities lack the financial and human resources necessary to meet advanced cybersecurity requirements, making compliance more challenging.

It could be argued that SMEs and start-ups may benefit from support measures such as guidance documents, helpdesks, and simplified documentation obligations.[174] According to article 33 of the act, Member States must support these enterprises and microenterprises through awareness campaigns, dedicated advisory channels, and assistance with testing and conformity assessments, including the use of regulatory sandboxes for innovative products. The Commission provides additional guidance, promotes available financial support, and establishes a simplified technical documentation format to help smaller enterprises comply with CRA requirements without undue administrative or financial burden.[175]

Practically, the CRACoWi (Cyber Resilience Act Compliance Wizard) initiative has been launched to provide a structured, step-by-step digital tool that guides SMEs through the CRA's compliance process. Funded under the Digital Europe Program and supported by the European Cybersecurity Competence Center, the CRACoWi project commenced on 1 September 2024 and aims to facilitate practical and accessible compliance for smaller businesses.[176]

Despite this promising initiative, significant economic challenges remain, and Member States must adopt comprehensive strategies to support SMEs enterprises in meeting CRA obligations. Such strategies should account for the size, resources, and sector-specific characteristics of each entity to ensure that compliance is both feasible and proportionate.

Another significant challenge in the implementation of the CRA concerns its interplay with the NIS2 Directive. While both instruments are designed to function as complementary

[173] Ibid., Recital 36. See also European Commission, Commission Staff Working Document – Executive Summary of the Impact Assessment Report Accompanying the Proposal for a Regulation for the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020, SWD(2022) 283 final, 15 September 2022, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52022SC0283 (Accessed 16 November 2025).
[174] Taylor Wessing, The Cyber Resilience Act – EU-Wide Requirements for the Cybersecurity of Products, 3 November 2025, available at: https://www.taylorwessing.com/en/insights-and-events/insights/2025/11/cyber-resilience-act-overview (Accessed 17 November 2025).
[175] Ibid., Article 33.
[176] CRACoWi: Cyber Resilience Act Compliance Wizard, available at: https://www.cracowi.eu/ (Accessed 20 Spetember 2026).

frameworks, their relationship has generated debate regarding potential overlaps and resulting uncertainty for regulated actors

Scholars argue that NIS2 imposes cybersecurity obligations on essential and important entities, whereas the CRA fills a critical regulatory gap by ensuring that the digital products underpinning these services are secure by design and maintained throughout their lifecycle; on this view, their interaction is mutually reinforcing, particularly in supply-chain security, vulnerability disclosure, and incident reporting, where CRA obligations feed into NIS2's coordination mechanisms through ENISA and national CSIRTs.[177] Other scholars highlighted that, together, the CRA and NIS2 play a vital role in strengthening consumer confidence and fostering user trust in digital technologies.[178]

On the other hand, other scholars caution that the CRA and NIS2 may create overlapping or inconsistent requirements for digital sectors, with concerns arising in areas like incident reporting and supply-chain responsibilities. This stems from the fact that the CRA focuses on product-level security, while NIS2 governs network and service-level resilience, a division that may complicate coordination between manufacturers and service providers.[179] In this context, Burri and Zihlmann note that "The CRA does provide also explicit guidance on its interplay with certain existing pieces of legislation", highlighting that while some clarification exists, practical coordination challenges may remain.[180]

In addition to above mentioned challenges, The CRA imposes several practical difficulties that stem from the inherent tension between creating a broad regulation and providing actionable guidance for manufacturers. A primary challenge is the ambiguous mandate to deliver products "without any known exploitable vulnerabilities", a requirement that is practically unfeasible as it fails to distinguish between critical vulnerabilities that pose immediate risks and minor, low-impact flaws, potentially forcing manufacturers to halt production indefinitely.[181]

[177] SCHMITZ-BERNDT – COLE, 2022, p.13.
[178] KHURSHID et al., 2022, p.129932.
[179] CHIARA, 2022, p.270.
[180] BURRI – ZIHLMANN, 2023, p. B20.
[181] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act). Annex I, Part I, point 2(A).

Furthermore, the requirement to "limit attack surfaces" remains critically undefined, leaving manufacturers of complex digital products like IoT ecosystems uncertain about how to substantiate compliance, especially regarding the security of external interfaces and inter-device communication.[182]

Additionally, while the provision of security updates is sometimes misconstrued as being capped at a rigid five-year period, the CRA establishes five years as a statutory minimum baseline Under Article 13(8) of the act , the required "support period" must be at least five years, or extend to correspond with the product's expected period of use if that lifetime is longer.[183] This creates a practical difficulty for manufacturers of long-lifecycle products, as the legally mandated support period may be substantially shorter than the period during which the product remains in active use.[184] For example, a smart thermostat or an industrial sensor with an expected lifespan of ten years would receive mandatory updates for only five years, potentially leaving users exposed to unpatched vulnerabilities for the remaining operational life of the device.

III.1.5 Cyber Solidarity Act

In response to the sharp increase in cybersecurity incidents reported by ENISA throughout late 2023 and the first half of 2024,[185] the EU recognized the urgent need for a coordinated supranational approach to cyber threats. These threats, targeting both public institutions and critical infrastructure ahead of the European Parliament elections, underscored the limitations of fragmented national responses and the need for stronger collective mechanisms for detection, preparedness, and coordinated response.[186]

Therefore, the EU adopted Regulation 2025/38, known as the Cyber Solidarity Act, on 19 December 2024, which was published in the Official Journal on 15 January 2025 and entered into force on 4 February 2025. [187] The Act establishes a framework for collective prevention,

[182] SHAFFIQUE, 2024, p.13.
[183] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), Article 13(8).
[184] SHAFFIQUE, 2024, p.8.
[185] European Union Agency for Cybersecurity, ENISA Threat Landscape 2024, 19 September 2024, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (Accessed 19 November 2025).
[186] VILLANI, 2025, p.485.
[187] European Parliament and Council of the European Union, Regulation (EU) 2025/38 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act).

preparedness, and response to large-scale cyber incidents, consolidating operational capabilities, promoting crisis management cooperation, and ensuring timely support to Member States, thereby reflecting European solidarity in the cyber domain.[188]

To this extent, the act has established main four features, the first one is cybersecurity alert system as a voluntary, pan-European network of National and Cross-Border Cyber Hubs aimed at strengthening the Union's capacities for detecting, analyzing, and processing cyber-threat information.

The mechanism institutionalizes structured collaboration with established EU cybersecurity entities, promoting the aggregation and production of actionable threat intelligence via sophisticated technical tools, alongside the issuance of early-warning alerts and regulatory recommendations to bolster joint detection and multi-jurisdictional situational awareness. The deployment of this infrastructure is financially sustained through the Digital Europe Program, securing the necessary operational and technological scaling across the internal market.[189]

The second feature of the Act is the establishment of the Cybersecurity Emergency Mechanism, which aims to reinforce the Union's overall resilience and to mitigate, in a spirit of solidarity, the immediate impacts of significant and large-scale cybersecurity incidents.[190] The Mechanism is activated upon request by Member States and is designed to operate in a complementary manner to national efforts in preparing for, responding to, and recovering from cyber incidents.[191] Its implementation relies primarily on the European Cybersecurity Competence Center (ECCC), which coordinates the delivery of most operational actions at Union level.

At the same time, specific components, which are most notably those relating to the EU cybersecurity reserve, are carried out jointly by the commission and ENISA to ensure a swift and coordinated response.[192] Furthermore, the emergency mechanisms encompass preparedness testing for highly critical sectors, response and recovery support through trusted service

[188] European Commission, "EU Cyber Solidarity Act", Digital Strategy, available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity (Accessed 19 November 2025).
[189] European Parliament and Council of the European Union, Regulation (EU) 2025/38 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act), Article 3.
[190] Ibid., Article 10(1).
[191] Ibid., Article 10(2).
[192] Ibid., Article 10(4).

providers,[193] and mutual assistance measures between Member States, thereby forming a comprehensive emergency framework.[194]

A scholar such as Villani has argued that the SolarWinds incident in 2020,[195] demonstrated the structural gaps in the EU's pre-2025 cyber-response framework, noting that had the Cyber Solidarity Act been in force at the time, it would have enabled a far more coordinated and rapid deployment of cross-border support mechanisms.[196] She observes that the Act's emergency tools could have reduced the fragmentation that characterized the EU's response in 2020. Indeed, this incident underscores the value of a solidarity-based model capable of mobilizing Union-level resources when large-scale cyber intrusions occur.

The third feature of the Act is the establishment of the European Cybersecurity Incident Review Mechanism, which enables ENISA, upon request from the Commission or European Cyber Crisis Liaison Organization Network (EU-CyCLONe), to review and assess significant or large-scale cybersecurity incidents with the support of the CSIRTs network and the approval of affected Member States.[197]

The mechanism involves consultation with a wide range of stakeholders, including Member States, Union institutions, industry actors, and affected entities, to ensure comprehensive feedback and accountability.[198] ENISA prepares an incident review report that analyzes causes, exploitable vulnerabilities, and lessons learned, while ensuring compliance with Union and national law and anonymizing sensitive data where requested.[199] The report may also include recommendations, best practices, and guidance to strengthen the Union's overall cybersecurity posture.[200]

---

[193] Ibid., Articles (11,12,13).
[194] Ibid., Article 18.
[195] Zscaler, What Is the SolarWinds Cyberattack?, available at: https://www.zscaler.com/resources/security-terms-glossary/what-is-the-solarwinds-cyberattack (Accessed 23 November 2025).
[196] VILLANI, 2025, p.493.
[197] European Parliament and Council of the European Union, Regulation (EU) 2025/38 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act), Article 21(1).
[198] Ibid., Article 21(2).
[199] Ibid., Article 21(3).
[200] Ibid., Article 21(4).

This review mechanism advances the EU cybersecurity framework by filling a gap left by earlier legislation such as the NIS2 Directive and the CRA, as none of which established a structured post-incident review procedure. Therefore, the act is regarded as the first comprehensive EU-level mechanism covering pre-incident, during-incident, and post-incident stages.[201]

The fourth feature of the Act is the establishment of the EU Cybersecurity Reserve, which provides rapid support to Member States, Union institutions, and digital Europe associated program (DEP) -Associated third countries during significant or large-scale cybersecurity incidents.[202] The Reserve relies on a pool of trusted managed security service providers (MSSPs), selected according to rigorous technical, operational, and security criteria, ensuring high-quality and reliable services across all Member States.[203] Its services include incident response, recovery support,[204] and, where pre-committed services are unused, preparedness activities such as training and exercises.[205]

The Commission holds overall responsibility for the implementation, supervision, and prioritization of the Reserve, while ENISA may be entrusted with its operation and administration, including mapping service needs and coordinating requests.[206] By formalizing access to expert technical support and enabling deployment in DEP-associated third countries, the EU Cybersecurity Reserve strengthens the Union's operational resilience and helps to address disparities in national cybersecurity capacities.[207]

However, while the Act represents an advanced and forward-looking step toward enhancing cybersecurity across the Union, it may nevertheless encounter several significant challenges. The first concerns are related to the voluntary nature of the European Cybersecurity Alert System, which being grounded in the need to respect Member States' national security prerogatives under Article 4(2) of the act risks generating fragmented participation and uneven

[201] DEWI – NUGRAHANI, 2024, p.189.
[202] European Parliament and Council of the European Union, Regulation (EU) 2025/38 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act), Article 14 (1,3).
[203] Ibid., Article 17(1,2),
[204] Ibid., Article 17(2)(k).
[205] Ibid., Article 14(2).
[206] Ibid., Article 14(4,6).
[207] Ibid., Articles (15,16).

capabilities throughout the Union,[208] echoing the shortcomings observed in the voluntary EU cybersecurity certification schemes.[209]

This challenge is further exacerbated by the system's interaction with existing EU cyber structures, where overlapping mandates and insufficiently delineated responsibilities may lead to duplicated efforts and inconsistent information flows. As national CSIRTs operate under strong domestic authority while Cross-Border Cyber Hubs pursue supranational objectives, maintaining trust, interoperability, and coherent reporting standards becomes inherently difficult, potentially undermining the overall effectiveness of the system.

The second challenge relates to the multi-actor governance structure of the cybersecurity emergency mechanism, which may create coordination frictions during time-sensitive cybersecurity incidents. Responsibilities are divided between ECCC, handling most operational actions, and the commission and ENISA, overseeing the EU cybersecurity reserve, with each actor operating under distinct mandates, procedures, and timelines. This complexity could hinder the prompt and coherent deployment of support, potentially undermining the Mechanism's overall effectiveness.

The third challenge is related to the requirement for Member State approval and broad stakeholder consultation within the European Cybersecurity incident review mechanism,[210] which, while ensuring legitimacy and trust, may slow the issuance of actionable recommendations during fast-moving cyber incidents. Collecting input from multiple Member States, CSIRTs, industry actors, and affected entities can create delays, particularly when national priorities, security classifications, or resource constraints differ.

Furthermore, while the Regulation's consultation requirements facilitate information-sharing and strengthen cyber-threat intelligence exchanges,[211] they also introduce political and sovereignty sensitivities. The expectation that Member States disclose sensitive data or coordinate strategic assessments may create reluctance, particularly where cybersecurity intersects with core

[208] Ibid., Article 3(1).
[209] European Parliament and Council of the European Union, Cybersecurity Act No. 2019/881. Article 56(2).
[210] European Parliament and Council of the European Union, Regulation (EU) 2025/38 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act), Article 21(2).
[211] DEWI – NUGRAHANI, 2024, p.192.

national-security competences. These dynamics illustrate how efforts to institutionalize solidarity in cyberspace can simultaneously expose underlying tensions in EU cybersecurity governance.

In emergent threat scenarios, such delays risk reducing the effectiveness of mitigation measures and limiting the mechanism's agility in responding to evolving incidents. The timelines established for ENISA to conduct reviews and deliver reports provide a structured framework to mitigate these delays, ensuring that lessons learned and recommendations are issued within a predictable and manageable period.

Another significant challenge concerns the dependency on private MSSPs, which may expose the EU cybersecurity reserve to risks related to availability, commercial interests, and conflicts of interest. While MSSPs are vetted for technical competence and security standards, their limited number and pre-committed service capacity could restrict the reserve's ability to respond to multiple or simultaneous incidents across Member States. Additionally, differences in national legal frameworks, data protection requirements, and operational protocols may complicate cross-border deployment, particularly to DEP-associated third countries.

III.2 Complementary Cybersecurity Legislation

III.2.1 General Data Protection Regulations (GDPR)

Cybersecurity and data protection are closely interconnected in the digital environment, as the protection of personal data increasingly depends on appropriate technical and organizational safeguards against unauthorized access, alteration, loss, and other security incidents.[212] Therefore, the EU enacted the GDPR,[213] which took effect on 25 May 2018, replacing the 1995 Data Protection Directive (DPD).[214]

The GDPR applies to processing activities within the scope defined by Article 3(1). Under this provision, the Regulation applies to the processing of personal data carried out in the context

[212] CATE et al., 2017, p.74.
[213] European Parliament and Council of the European Union, Regulation No. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).
[214] European Parliament and Council of the European Union, Directive No. 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. See also Article 94 of the GDPR.

of the activities of an establishment of a controller or processor in the Union, regardless of whether the processing itself takes place within the Union.[215]

Article 3(2) further extends its territorial reach to certain processing activities undertaken by organizations established outside the EU, particularly where they offer goods or services to individuals in the Union or monitor their behavior.[216] This extraterritorial scope gives the GDPR significant regulatory influence beyond the Union and enables certain European data-protection and security requirements to affect organizations operating in international digital markets.

Although GDPR is primarily a data protection instrument rather than a dedicated cybersecurity law, it forms an important component of the EU's broader cybersecurity governance framework. The Regulations connect data protection with cybersecurity principally through its requirements concerning security and accountability. Article 32 requires controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks associated with processing personal data. These measures may include encryption, pseudonymization, confidentiality, integrity, availability, resilience, and the capacity to restore access to personal data following an incident.[217] Accordingly, cybersecurity measures become a direct element of statutory compliance where personal data are processed.

The enforceability of these requirements is demonstrated through regulatory practice. In 2020, the German Data Protection Authority of Baden-Württemberg imposed a €1.24 million fine on AOK Baden-Württemberg in connection with inadequate technical and organisational measures concerning the processing of personal data. Although security measures had been implemented, the authority considered them insufficient in the circumstances, following the unlawful use of personal data in marketing activities.[218] The case illustrates that Article 32 is not merely aspirational: inadequate technical and organizational safeguards may constitute an enforceable data-protection violation where they contribute to unlawful or insufficiently protected processing.

---

[215] European Parliament and Council of the European Union, Regulation No. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), Article 3(1).
[216] Ibid., Article 3(2).
[217] European Parliament and Council of the European Union, Regulation No. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), Article 32.
[218] Fieldfisher, 500 unlawful marketing e-mails with insufficient consent, available at: https://www.fieldfisher.com/en/insights/500-unlawful-marketing-e-mails-with-insufficient-c (Accessed 25 Nov. 2025).

Nevertheless, the GDPR does not comprehensively regulate the cybersecurity of digital products or impose general cybersecurity obligations on manufacturers and developers. Its principal security obligations attach to controllers and processors in the context of personal-data processing. This limitation is particularly significant where cybersecurity risks arise from the design, development, or supply of digital products rather than from the processing of personal data itself.[219] The distinction illustrates the complementary nature of EU cybersecurity legislation: while the GDPR addresses security risks associated with personal-data processing, horizontal product-security instruments such as the CRA extend regulatory requirements to the cybersecurity of products with digital elements.

The preventive dimension of the GDPR is further reinforced by Article 25, which establishes data protection by design and by default. The provision requires controllers to integrate appropriate data-protection safeguards into processing activities and system design from the outset, rather than relying exclusively on remedial measures after a breach has occurred.[220] Although Article 25 is directed primarily toward data protection rather than general cybersecurity, it contributes to the preventive dimension of EU digital governance by encouraging security and privacy considerations to be incorporated into organizational and technological processes at the design stage.

The GDPR also establishes specific obligations concerning the response to personal-data breaches. Articles 33 and 34 require notification of certain personal-data breaches to the competent supervisory authority and, where the relevant conditions are met, communication of the breach to affected data subjects.[221] These obligations complement the incident-reporting mechanisms established under EU cybersecurity legislation. In particular, Article 23 of NIS2 establishes reporting obligations for significant cybersecurity incidents affecting entities within its scope.[222]

[219] HESSEL – REBMANN, 2020, p.30.
[220] European Parliament and Council of the European Union, Regulation No. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), Article 25.
[221] European Parliament and Council of the European Union, Regulation No. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), Articles (33(1),34(1)).
[222] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 23.

Although the GDPR and NIS2 pursue different regulatory objectives, their respective incident-reporting requirements may operate in parallel where a cybersecurity incident also results in a personal-data breach. This creates an important point of interaction between data-protection and cybersecurity governance.

The GDPR therefore occupies a complementary position within the EU cybersecurity governance architecture by linking the protection of personal data with the security of information systems. Its requirements concerning security, prevention, accountability, and breach response demonstrate how cybersecurity obligations may arise through interconnected areas of EU regulation. At the same time, the GDPR's focus on personal-data processing illustrates the limits of data-protection law as a comprehensive cybersecurity framework, thereby reinforcing the need for complementary instruments addressing broader organizational, network, system, and product-security risks.

III.2.2 Artificial Intelligence Act (AIA)

The rise of AI technology is viewed as one of the most significant technological developments of the past decade and among the most advanced achievements of the modern technological era. It has refined nearly every function that machines perform and expanded the boundaries of what they can accomplish. Some scholars even consider it one of humanity’s greatest creations that surpasses much of our own understanding.[223]

AI is now becoming an integral part of modern cybersecurity systems. Today, AI helps detect and prevent spam, phishing attempts, and various forms of online fraud. For example, MasterCard uses AI-driven decision intelligence to analyze consumer behavior patterns and identify potentially fraudulent transactions.[224]

Despite its growing role in defense, AI itself can introduce new cybersecurity risks, as these systems may contain vulnerabilities that can be exploited by malicious actors. Recognizing these risks, the EU has integrated cybersecurity requirements directly into the statutory framework of

[223] ANSARI et al., 2022, p.85.
[224] WELUKAR – BAJORIA, 2021, p.490.

the AIA, which was published in the Official Journal on 12 July 2024 and entered into force on 1 August 2024.[225]

Recital 76 of the AIA highlights that cybersecurity is essential to ensure AI systems remain resilient against malicious attempts to alter their behavior, performance, or compromise their security. It further recognizes that cyberattacks may exploit AI-specific assets, such as training datasets and trained models, as well as vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure. Accordingly, providers of high-risk AI systems should take appropriate cybersecurity measures, taking the underlying ICT infrastructure into account where appropriate.[226]

Article 15 of the act mandates that high-risk AI systems must be designed to ensure an appropriate level of accuracy, robustness, and cybersecurity throughout their lifecycle.[227] These systems are required to remain resilient against errors, faults, or inconsistencies arising internally or from the environment in which the system operates, with technical and organizational measures, including redundancy or fail-safe solutions, to maintain consistent performance.[228]

In this context, scholars have noted that the objectives of robustness and cybersecurity, while related, address different types of threats. Robustness is primarily concerned with resilience against errors, faults, inconsistencies, and other disruptions affecting system performance, whereas cybersecurity focuses specifically on attempts by unauthorized third parties to exploit vulnerabilities or compromise the system.[229]

Although both aim to maintain reliable system performance, the nature of the protections they require differs: robustness safeguards high-risk AI systems against technical or operational disruptions, while cybersecurity seeks to prevent and mitigate malicious attacks that could impair system functionality.

---

[225] European Parliament and Council of the European Union, Regulation (EU) No. 2024/1689 harmonized rules on artificial intelligence (Artificial Intelligence Act).
[226] Ibid., Recital 76.
[227] Ibid., Article 15(1).
[228] Ibid., Article 15(4).
[229] Nolte Henrik, Rateike Miriam, Finck Michèle, Robustness and Cybersecurity in the EU Artificial Intelligence Act. 2025. Available at: https://blog.genlaw.org/pdfs/genlaw_icml2024/4.pdf (Accessed 16 Nov. 2025).

Building on these principles, AI systems that continue to learn post-deployment require additional safeguards to prevent biased outputs from influencing future operations. High-risk AI systems must be protected against cyberattacks, including attempts by unauthorized third parties to manipulate their use, outputs, or performance. Specific measures should address AI-specific vulnerabilities such as data poisoning, model poisoning, adversarial attacks, and confidentiality breaches, with technical solutions appropriate to the risks posed by each system.[230]

To facilitate compliance, high-risk AI systems that have been certified or for which a statement of conformity has been issued in accordance with CSA, are presumed to comply with the cybersecurity requirements of Article 15 to the extent that the relevant certification or statement of conformity covers those requirements.

While this mechanism allows existing recognized certifications to serve as evidence of compliance, it also highlights a structural limitation: the AIA does not construct an autonomous, AI-specific definition of cybersecurity.[231] Instead, it relies in part on the broader EU cybersecurity certification framework established under CSA, including ENISA's role in the development of European cybersecurity certification schemes.

However, a key limitation remains: the availability of cybersecurity certification schemes specifically addressing the particular characteristics and risks of AI systems has remained limited. As a result, the interplay between the two acts is conceptually strong but its practical application through certification mechanisms may remain incomplete where existing schemes do not adequately address AI-specific cybersecurity risks. [232] This highlights a crucial governance gap between the substantive cybersecurity obligations imposed by the AIA and the availability of specialized certification mechanisms capable of demonstrating compliance with those obligations.

The AIA does not interact solely with the CSA; it also intersects with other cybersecurity legislation, most notably the CRA. This interplay arises particularly where a product with digital elements also incorporates or constitutes a high-risk AI system. In such cases, compliance with the

[230] European Parliament and Council of the European Union, Regulation (EU) No. 2024/1689 harmonized rules on artificial intelligence (Artificial Intelligence Act), Article 15(5).
[231] Ibid., Article 42(2).
[232] Hans Graux et al., Interplay between the AI Act and the EU Digital Legislative Framework, European Parliament Study, 2025, p. 58, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778575/ECTI_STU(2025)778575_EN.pdf (Accessed 27 Nov.2025).

CRA's essential cybersecurity requirements, such as secure-by-design requirements, vulnerability handling, and lifecycle security, supports the fulfilment of the cybersecurity requirements of the AIA through an expressly established conformity mechanism, rather than merely providing supplementary safeguards.

The CRA provides horizontal cybersecurity requirements for products with digital elements, which are relevant where AI systems are incorporated into such products because many AI-related cybersecurity risks may also arise from vulnerabilities in the wider digital environment. This relationship is reflected not only in Recital 76 and Article 15 of the AIA, but also expressly in Article 12 of the CRA. Under Article 12(1) CRA, products with digital elements that are classified as high-risk AI systems are deemed to comply with the cybersecurity requirements of Article 15 AIA where the specified CRA requirements are fulfilled and the required level of cybersecurity protection is demonstrated in the EU declaration of conformity.[233]

This interaction is further confirmed by Article 42(3) of AIA, which provides that high-risk AI systems falling within the scope of the CRA and satisfying the conditions of Article 12(1) CRA are deemed to comply with the cybersecurity requirements of Article 15 AIA.[234] The current legal framework therefore does not treat the CRA as merely an external or supplementary cybersecurity instrument; rather, it establishes a direct legal mechanism through which CRA compliance can contribute to compliance with the AIA's cybersecurity requirements.

This development is significant from a governance perspective. Although Article 42(2) AIA retains the presumption of conformity associated with cybersecurity schemes established under CRA, Article 42(3) expressly accommodates the CRA. The relationship therefore demonstrates an emerging form of regulatory interoperability between horizontal product cybersecurity requirements and AI-specific cybersecurity obligations, reducing the risk of entirely separate conformity assessment processes while preserving the distinct regulatory objectives of the two instruments.[235]

---

[233] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act). Article 12(1).
[234] European Parliament and Council of the European Union, Regulation (EU) No. 2024/1689 harmonized rules on artificial intelligence (Artificial Intelligence Act), Article 15.
[235] European Parliament and Council of the European Union, Regulation (EU) No. 2024/1689 harmonized rules on artificial intelligence (Artificial Intelligence Act), Article 42(3). See also European Parliament and of the Council, Regulation (EU) 2026/1744 of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU)

The AIA also interacts with the NIS2 Directive, with the interplay arising when an organization falls simultaneously under the scope of both instruments. In such cases, the entity must fulfil its organizational cybersecurity obligations under NIS2 while ensuring that its high-risk AI systems comply with the technical cybersecurity and robustness requirements set out in Article 15 AIA.[236]

This creates a dual regulatory compliance layer, whereby NIS2 governs the security of the broader organizational environment, and the AIA governs the security of the AI systems themselves. From an administrative oversight perspective, this overlap creates the potential for a dual reporting burden in incident management, with different authorities and reporting timelines depending on the applicable legal obligations and national implementation, potentially imposing significant administrative challenges on essential and important entities.

III.2.3. The Digital Operational Resilience Act (DORA)

DORA was formally adopted on 14 December 2022 and entered into force on 16 January 2023 with full applicability from 17 January 2025.[237] It aimed to ensure that financial entities are equipped to withstand, respond to, and recover from ICT-related disruptions, ultimately safeguarding the stability and integrity of the European financial system.

DORA established a harmonized statutory framework designed to strengthen the legal governance of digital operational resilience across the EU.[238] The act introduced comprehensive and binding requirements for ICT-risk management, incident reporting, operational resilience testing, and the oversight of critical third-party ICT service providers, thereby addressing the growing frequency and severity of cyber threats targeting the financial sector.

DORA encompasses a broad personal scope, applying to virtually all supervised financial entities, including traditional institutions such as banks, insurers, and investment firms, as well as

2023/1230 as regards the simplification of the implementation of harmonized rules on artificial intelligence (Digital Omnibus on AI).

[236] Hans Graux et al Interplay between the AI Act and the EU Digital Legislative Framework, European Parliament Study, 2025, p. 65, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778575/ECTI_STU(2025)778575_EN.pdf (Accessed 27 Nov.2025).

[237] European Parliament and Council of the European Union, 2022, Regulation No. 2022/2554 on digital operational resilience for the financial sector (DORA), Article 64(2).

[238] Ibid., Article 6.

emerging actors, including payment and e-money institutions, trading venues, crypto-asset service providers, and issuers of asset-referenced tokens.[239]

This comprehensive coverage is intended to ensure that financial entities subject to DORA implement fundamental cyber-resilience measures, with proportionate requirements and, for specified categories of financial entities, a simplified ICT-risk management framework.[240] Statutory auditors and audit firms, however, are not currently within the scope of DORA. Nevertheless, Article 58(3) provides for a review of whether strengthened digital operational resilience requirements should apply to them.[241]

DORA encompasses several key features, among which the most significant is the establishment of a comprehensive ICT-risk management framework. Under this framework, financial firms are required to implement an internal governance and control system to effectively manage all ICT-related risks, ensuring that cyber resilience is embedded within overall operational processes.[242]

The management body of the financial entity bears ultimate statutory responsibility for the governance, implementation, and oversight of the ICT-risk management framework.[243] This framework must define documented strategies, policies, protocols, and technical tools to protect information and physical ICT assets.[244] Furthermore, financial entities are required to identify, classify, and document all ICT-supported business functions, information assets, and interdependencies.[245] They must systematically assess operational risks, deploy preventive controls, maintain continuous monitoring mechanisms, and formulate business continuity and reduce the risk that ICT-related disruptions may generate wider consequences for the financial system.[246]

Another central feature of DORA concerns the regulation and supervision of ICT third-party risk arising from financial entities' reliance on external service providers.[247] The Regulation

[239] Ibid., Article 2(1).
[240] Ibid., Article 16.
[241] Ibid., Article 58(3).
[242] Ibid., Article 6.
[243] Ibid., Article 5.
[244] Ibid. Article 6(1,4).
[245] Ibid., Article 8.
[246] Ibid., Articles (9,10,11,12,13).
[247] Ibid., Article 28(1).

requires financial firms to integrate ICT third-party risk into their overall ICT risk management framework, while remaining fully responsible for compliance and operational resilience, irrespective of outsourcing arrangements.[248]

To this end, DORA imposes obligations relating to pre-contractual due diligence, risk assessments, contractual safeguards, ongoing monitoring, and the development of exit and transition strategies for critical ICT services.[249] In addition, DORA introduces a novel EU-level oversight framework for critical ICT third-party service providers, granting Lead Overseers among the European Supervisory Authorities (ESAs) direct supervisory powers over such providers, including powers of investigation and inspection, thereby mitigating systemic concentration risks across the financial system as a whole.[250]

Despite its comprehensive design, DORA's ICT-risk management framework faces several practical challenges that may affect its effective implementation. The multi-level structure of EU financial supervision may create challenges of coordination and consistency in the application of ICT-risk management requirements across Member States, potentially undermining supervisory convergence and regulatory certainty.[251]

Moreover, the interaction between national competent authorities and EU-level supervisory structures may create duplication, increase compliance costs, and complicate supervisory coordination, particularly in relation to ICT third-party risk. Accordingly, the effectiveness of DORA depends not only on the substantive obligations imposed by the Regulation, but also on the capacity of European and national supervisory structures to coordinate their functions and ensure consistent implementation.

Chapter IV: The Jordanian Legal and Regulatory Framework for Cybersecurity

IV.1 Core Cybersecurity Legislation

IV.1.1 Cybersecurity Law

In recent decades, cybersecurity threats have emerged as one of the most significant challenges facing states, including developing countries such as Jordan, owing to their increasing

[248] Ibid., Article 28(2).
[249] Ibid., Articles (29,30).
[250] Ibid., Articles (31,32,33,34,35,36).
[251] BUTTIGIEG – BRUNELLI, 2024, p.20.

sophistication, scale, and transnational nature. These threats no longer merely target isolated national information systems; rather, they increasingly undermine Jordan's national security, economic stability, and critical infrastructure.

Despite the adoption of advanced technical and regulatory measures by national financial and institutional entities, the frequency and impact of cybersecurity threats have continued to escalate, particularly during the second decade of the twenty-first century. This escalation has exposed the limitations of national entities in combating such threats when relying solely on individual or sector-specific efforts.[252]

Consequently, the Jordanian government has recognized the necessity of establishing a comprehensive legal framework and strengthening international cooperation to effectively prevent, detect, and respond to cybersecurity threats. In this context, Jordan enacted Cybersecurity Law No. 16 of 2019 as a cornerstone of its national legislation aimed at enhancing cybersecurity governance and protecting its digital environment.[253]

The legislative intent behind the enactment of Cybersecurity Law is clearly reflected in its explanatory memorandum, which indicates that the Jordanian legislature sought to adopt an *ex-ante* framework rather than a purely punitive or substantive legislative approach. The primary objective of the law is to protect the Kingdom from cybersecurity threats and incidents by establishing a national cybersecurity system administered by a specialized authority capable of addressing threats targeting information systems and critical infrastructure.[254]

Furthermore, the law aims to enhance the overall level of national security for both institutions and individuals by developing national capacities for monitoring, early warning, and response to cybersecurity incidents, while mitigating the potential damages arising from such incidents. Beyond security considerations, the law aims to create a secure and attractive digital environment for investment, thereby contributing to the strengthening of the national economy, particularly in light of the rapid advancement of information systems, critical infrastructure, and the expanding scope of electronic government services.

[252] SVIATUN et al., 2021, p.751.
[253] Jordan, Cybersecurity Law No. 16 of 2019.
[254] AL-KASASSBEH et al. 2023, p.357.

In order to achieve these objectives, the Jordanian legislator did not confine the law to general policy declarations, but instead structured it around a coherent and integrated and comprehensive system that combines conceptual clarity, institutional organization, and enforceable mechanisms. Accordingly, the provisions of the law may be analytically examined through three interrelated dimensions.

The first concerns the conceptual and normative foundations of the law, as reflected in its definitional provisions and the scope of its application. The second dimension is the institutional architecture established by the law, particularly the creation and functions of the National Cybersecurity Council and the NCSC as the core bodies responsible for cybersecurity governance. The third one relates to the executive, regulatory, and enforcement mechanisms adopted by the law, including obligations imposed on public and private entities, incident response arrangements, licensing regimes, and the system of administrative measures and sanctions designed to ensure compliance and effectiveness.

IV.1.1.1 Conceptual Framework and Scope of Application

Prior to the enactment of the Jordanian Cybersecurity Law, cybersecurity was primarily addressed at the doctrinal level, and several definitions were proposed by Arab legal scholars. One scholar defined cybersecurity as "an activity that ensures the protection of human and financial resources associated with communication and information technologies and guarantees the possibility of reducing loss and damage; where risks and threats materialize, it allows the situation to be restored as quickly as possible so that the production process does not cease and damage does not become permanent".[255]

While this definition highlights the role of cybersecurity in risk mitigation and operational continuity, it remains largely confined to economic and financial considerations, without sufficiently encompassing other essential dimensions such as national security, critical infrastructure protection, or societal and individual rights.

Another scholar defined cybersecurity as "Defensive techniques or security measures adopted to detect and thwart potential intruders".[256] Although this definition emphasizes the technical and preventive aspects of cybersecurity, it adopts a narrow operational perspective as it

[255] AL-KASASSBEH et al. 2023, p.352.
[256] MOSTAFA, 2022, p.722.

conceptualizes cybersecurity primarily as a set of technical defense mechanisms, limiting its scope to intrusion detection and prevention and failing to account for the broader functions of cybersecurity, such as resilience, coordinated response, and sustained system stability in the face of evolving threats.

As previously noted, the Jordanian Cybersecurity Law defines cybersecurity as "The measures taken to protect information systems, networks, and critical infrastructure from cybersecurity incidents, and the ability to restore their functioning and continuity, whether such incidents result from unauthorized access, misuse, failure to follow security procedures, or deception leading to such breaches".[257] Although this definition is not without shortcomings, it nonetheless represents a progressive step toward the regulation and standardization of legal digital terminology within Arab legal systems, particularly by adopting a comprehensive and functional approach to cybersecurity.

The definition of cybersecurity as articulated by the Jordanian legislator may be analytically construed as encompassing three essential constituent elements. The first element pertains to the operational measures adopted by relevant actors, including private corporations, governmental entities, and individuals.

The second element concerns the underlying objective of such measures, namely the protection and preservation of information systems, digital networks, and critical infrastructure. The third element relates to the nature of the risk addressed, specifically the occurrence or potential occurrence of cybersecurity incidents. These elements provide a useful framework for analyzing the scope and limitations of the law.

With regard to the first element, the operational component encompasses all actions taken by relevant actors to safeguard information and digital infrastructure. These measures include a wide range of technical, administrative, and procedural practices designed to prevent or mitigate threats posed by malicious actors, including hackers and cybercriminals. Such threats may take the form of malware, phishing, ransomware, data breaches, or other types of cyberattacks that compromise the confidentiality, integrity, or availability of information and systems.

[257] Jordan, Cybersecurity Law No. 16 of 2019, Article 2.

With respect to the second element, the protective objective, the law identifies the protection of information systems, networks, and critical infrastructure as its principal objective. Information systems consist of integrated components that collect, process, store, and transmit data to support decision-making processes electronically. Networks, in turn, represent interconnected devices, such as computers, servers, and other information systems, enabling the exchange of data across electronic platforms.[258] Ensuring the continuity of these systems and networks is essential not only for organizational operations but also for societal stability, particularly when such systems constitute critical infrastructure whose uninterrupted function is necessary to safeguard national security.

With regard to the third element, namely the risk dimension, the Jordanian law defines a cybersecurity incident as "an act or attack that poses a threat to data, information, information systems, networks, or associated infrastructure, requiring a response to stop it or mitigate its consequences".[259]

Although Article 2 of the Jordanian Cybersecurity Law expressly recognizes failures to follow security measures within its definition of cybersecurity, the separate definition of a cybersecurity incident refers to an "act or attack" without expressly clarifying the treatment of accidental technical failures, misconfigurations, or other non-malicious events. This drafting may create uncertainty regarding the scope of incidents covered by the statutory framework. [260]

Comparative regulatory instruments adopt broader and more expansive definitions of cybersecurity. For instance, the first EU NIS Directive defines a cybersecurity incident as "any event having an actual adverse effect on the security of network and information systems."[261] The subsequent NIS2 Directive expands on this definition, considering an incident as "an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information system."[262]

[258] Ibid.
[259] Ibid.
[260] OPDERBECK, 2016, p.935.
[261] European Parliament and Council of the European Union, Directive No. 2016/1148 on the Security of Network and Information Systems Across the Union (NIS Directive). Article 4(7).
[262] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 6(6).

European cybersecurity legislation explicitly recognizes that incidents stem from both adversarial attacks and non-adversarial system failures. Compared to European standards, the Jordanian statutory definition focuses predominantly on intentional or physical acts, creating a legislative gap regarding non-malicious technical risks.

While documented large-scale crises caused purely by human error remain limited in Jordan, law enforcement agencies—such as the Cybercrime Unit—frequently warn users against weak credentials and unpatched software.[263] Globally, research indicates that 39% of operational security risks relate directly to human behavior, and up to 95% of successful breaches involve human error.[264]

Despite this empirical evidence which demonstrates that human error constitutes a substantial proportion of cybersecurity incidents, the Jordanian legislator has not explicitly incorporated this dimension into the statutory definition of a cybersecurity incident. The current formulation, by framing the incident primarily as an "act or attack," implicitly emphasizes deliberate or externally driven conduct. This legislative approach risks excluding or minimizing incidents arising from negligent behavior, misconfiguration, weak authentication practices, or other unintentional failures, even though such factors represent a significant source of contemporary cyber risk. Consequently, the absence of an express reference to human error may limit the law's conceptual alignment with prevailing international standards and undermine a comprehensive risk-based approach to cybersecurity governance.

IV.1.1.2 The Regulatory and Institutional Nature of the Jordanian Cybersecurity Law

The Jordanian Cybersecurity Law No. 16 of 2019 reflects a deliberate legislative choice to adopt a predominantly regulatory and administrative governance model, rather than a substantive Criminal Law. This orientation is evident throughout the statute, which prioritizes organizational structures, compliance oversight, and operational coordination over technical coding specifications or criminal sanctions.

As one of the primary objectives of the law tis he establishment of an administrative governance framework defining the statutory mandates, regulatory powers, and institutional

[263] Roya News, Anti-Cybercrime Unit Warns Jordanians Against WhatsApp Fraud, 2020, available at: https://en.royanews.tv/news/58375 (Accessed 17 Feb. 2026).
[264] ALSHARIF et al., 2022, p.1153.

structure of the NCSC. In this regard, the law prioritizes coordination, continuous risk management, and compliance over punitive sanctioning. Although it provides for administrative measures in cases of non-compliance, these controls aim to compel adherence to security standards rather than assign criminal culpability.

This legislative philosophy demonstrates the Jordanian legislator's intention to classify the Cybersecurity Law as a regulatory instrument rather than a purely substantive or punitive statute. This approach finds a parallel in other regional jurisdictions that have established specialized administrative bodies for cybersecurity governance. For example, Qatar established its National Cyber Security Agency via Amiri Decision No. (1) of 2021, providing a targeted comparative model for strengthening cybersecurity through dedicated supervisory oversight and policy development.[265]

The decision to limit the Cybersecurity Law to an administrative framework raises a doctrinal question: Was confining the statute to regulatory rules appropriate, or should criminalization mechanisms have been integrated directly into its text?

From a legal theory perspective, legal norms are traditionally classified into substantive rules, which regulate rights, obligations, and prohibitions such as criminal law,[266] and procedural rules, which govern the mechanisms and processes for enforcing those rights and obligations, such as criminal procedure law.[267]

There is no constitutional or legislative bar in Jordan preventing the combination of substantive criminal prohibitions and administrative rules within a single statute. For instance, the Jordanian Electronic Crimes Law is fundamentally a substantive penal statute, yet it incorporates regulatory duties, such as Article 37 imposing compliance obligations on social media platforms.[268] Consequently, the Cybersecurity Law could have legally incorporated penal sanctions alongside its administrative provisions.

Nevertheless, it may be argued that many legal systems deliberately separate regulatory cybersecurity frameworks from criminal statutes. At the European level, the CSA does not include

[265] State of Qatar, Amiri Decision No. 1 of 2021 Establishing the National Cyber Security Agency.
[266] - AL-HUSSEINI – JASSIM, 2018, p.3.
[267] Ibid.
[268] Jordan, Electronic Crimes Law No. 17 of 2023, Article 37.

substantive criminal provisions, focusing instead on institutional and procedural rules.[269] Substantive criminalization of attacks against information systems is enacted separately under Directive 2013/40/EU. Maintaining this separation between *ex-ante* administrative governance and *ex-post* criminal sanctioning preserves procedural clarity and prevents administrative regulators from assuming judicial functions.[270]

IV.1.1.3 The Institutional Framework of Cybersecurity Governance in Jordan

IV.1.1.3.1 The National Cybersecurity Council: Strategic Oversight and Policy Direction

The Jordanian National Cybersecurity Council was formally established in early 2021 pursuant to article 3 of Cybersecurity Law No.16 of 2019.[271] The Council operates as the kingdom's highest strategic authority in the field of cybersecurity governance. its primary mandate is to support the establishment of a robust and comprehensive national cybersecurity system aimed at protecting the kingdom from potential cyber threats and attacks.

The Council is chaired by a president appointed by royal decree and comprises members representing key governmental and security institutions, including the Ministry of Digital Economy and Entrepreneurship, Central Bank of Jordan, the Jordanian Armed Forces, General Intelligence Directorate, Public Security Directorate, and the National Center for Security and Crisis Management. in addition, the Council of Ministers appoints three members upon the nomination of the Council president, two of whom must possess relevant expertise from the private sector. This composition reflects a deliberate effort to integrate both public and private sector perspectives within national cybersecurity decision-making.[272]

While this membership integrates public and private sector perspectives, the prominent representation of military, intelligence, and police bodies establishes a security-driven governance model. In contrast, jurisdictions such as the EU emphasize multi-stakeholder structures, where ENISA integrates Member States, industry representatives, civil society, and independent privacy authorities.[273] While Jordan's centralized architecture enhances operational coordination during

[269] European Parliament and Council of the European Union, Cybersecurity Act No. 2019/881.
[270] European Parliament and Council of the European Union, Directive 2013/40 on attacks against information systems.
[271] Jordan, Cybersecurity Law No. 16 of 2019, Article 3.
[272] Ibid.
[273] European Union Agency for Cybersecurity, ENISA Stakeholder Strategy 2026–2028, January 2026. https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Stakeholder%20Strategy%202026-2028.pdf (Accessed 27 Feb. 2026).

emergencies, it presents governance challenges regarding institutional balance and civilian supervisory oversight.

In terms of the Council's functions, it's responsible for approving national cybersecurity strategies, policies, and standards. It also endorses the plans and programs necessary for the NCSC to perform its duties, including initiatives related to regional and international cooperation. Furthermore, the Council reviews and adopts quarterly reports on the national cybersecurity situation, as well as the Center's annual activity report. to facilitate effective coordination, the Council is empowered to establish specialized coordination committees and to define their mandates, procedures, and decision-making mechanisms. Finally, the Council exercises financial oversight through the approval of the NCSC's annual budget.[274]

In practical application of its statutory mandate, the National Cybersecurity Council has recently exercised its strategic oversight functions through the adoption of the National Cybersecurity Strategy for the period 2025–2028.[275] This strategy constitutes a comprehensive national framework designed to support the efforts of the Hashemite Kingdom of Jordan, through the NCSC, in establishing an effective and resilient national cybersecurity ecosystem. The Center is tasked, in coordination with relevant national stakeholders, with the development of an executive program for the strategy and with overseeing the implementation of its associated policies, programs, and activities in accordance with defined timelines and performance indicators.

The strategy articulates Jordan's vision of building a secure, trusted, and resilient national cyberspace grounded in domestic capabilities and supportive of economic growth and societal well-being. This vision is pursued through four principal strategic objectives, supported by fourteen subsidiary goals, structured around clearly defined priorities.

These objectives include enhancing security and trust through data protection and the safeguarding of critical digital infrastructure and services; strengthening resilience to ensure service continuity in the face of cybersecurity governance; developing national capacities through skills enhancement, research support, and the adoption of emerging technologies; and promoting

[274] Jordan, Cybersecurity Law No. 16 of 2019, Article 4.
[275] Jordan, National Cybersecurity Center, National Cybersecurity Strategy 2025–2028, 2025, available at: https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/national_cybersecurity_strategy_2025-2028.pdf (Accessed 19 January 2026).

cooperation and partnerships at both the national and international levels to facilitate knowledge exchange and address evolving cybersecurity governance challenges.[276]

Ultimately, the National Cybersecurity Strategy seeks to position Jordan as a distinguished regional hub for cybersecurity, while securing the national digital environment and fostering a safe, innovation-driven ecosystem conducive to investment and aligned with the Kingdom's broader economic modernization and digital transformation agenda.

IV.1.1.3.2 The NCSC: Operational Authority and Regulatory Implementation

The establishment of the NCSC represents the core operational component of Jordan's cybersecurity framework. Created under Article 5 of the Cybersecurity Law,[277] the Center became operational in early 2021 as the primary administrative authority responsible for implementing national cybersecurity policies. Institutionally, the Center reports directly to the Prime Minister, reflecting the strategic priority assigned to digital risk management and national resilience.

Article 6(a) defines the overarching mandate of the Center as building, organizing, and maintaining a national cybersecurity system capable of safeguarding the Kingdom from cyber threats.[278] This objective extends beyond reactive threat mitigation to encompass the sustainability of critical infrastructure and the protection of digital assets.[279]

To fulfill this mandate, Article 6(b) confers upon the Center an extensive set of regulatory, operational, and coordination powers. First, the Center is entrusted with the development and enforcement of national cybersecurity strategies, policies, and standards, as well as the preparation of plans and programs necessary for their implementation. These instruments are subsequently submitted to the National Cybersecurity Council for approval, reinforcing a governance model that separates strategic policy oversight from operational execution.[280]

Second, the Center plays a central role in cybersecurity operations and incident response coordination. It provides technical support and advisory services to enhance the capacity of cybersecurity operations teams across both public and private sectors. In cases involving serious cybersecurity incidents, particularly those affecting critical infrastructure, the Center is

[276] Ibid.
[277] Jordan, Cybersecurity Law No. 16 of 2019, Article 5.
[278] Ibid., Article 6(a).
[279] AL-MUHAISEN et al., 2024, p.855.
[280] Jordan, Cybersecurity Law No. 16 of 2019, Article 6(b)(1).

empowered to coordinate national response efforts and intervene, when necessary, thereby ensuring a unified and timely response to threats.[281]

Third, the Center is responsible for establishing regulatory controls and risk classification mechanisms, including the classification of cybersecurity incidents according to their operational severity and systemic impact.[282] In addition, it regulates the cybersecurity services market by granting licenses to cybersecurity service providers based on specific technical, administrative, and financial requirements set out in implementing regulations.[283] This licensing function reflects the Center's dual role as both a market regulator and a supervisory authority.

Fourth, the Center serves as a national hub for information exchange and international cooperation. It facilitates the sharing of cybersecurity-related information and enters into agreements and memoranda of understanding with national, regional, and international organizations. This statutory function underscores the inherently transnational nature of cyber risks and aligns Jordan's administrative security governance with international best practices.[284]

Fifth, capacity building and awareness development constitute a core component of the Center's mandate. The Center designs and implements programs aimed at enhancing national cybersecurity expertise and raising awareness among institutions and the public regarding cybersecurity risks and preventive measures.[285] In parallel, the Center collaborates with academic institutions to support scientific research and innovation in cybersecurity, thereby contributing to the long-term development of national capabilities.[286]

In addition to these regulatory and administrative functions, the Center is vested with direct statutory enforcement and investigative powers. Under Article 13(a) of the Law, the President of the Center and authorized officials are granted judicial police authority empowering them to enter and inspect premises suspected of cybersecurity violations, inspect and seize electronic hardware

[281] Ibid., Article 6(b)(2).
[282] Ibid., Article 6(b)(3).
[283] Jordan, Instructions for the Classification of Cybersecurity Incidents for the Year 2023, issued pursuant to Clause (3) of Paragraph (b) of Article 6 of the Cybersecurity Law No. 16 of 2019, 2023, available at: https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/cyber_security_incidents_categorization_instructions_2023.pdf, (Accessed on 19 January 2025).
[284] Jordan, Cybersecurity Law No. 16 of 2019, Article 6(b)(5).
[285] Ibid., Article 6(b)(6).
[286] Ibid., Articles (6(b) (7,15)).

and information systems, and execute administrative enforcement measures against non-compliant entities.[287]

While these enforcement mechanisms enhance the Center's regulatory efficacy, they simultaneously raise fundamental legal concerns regarding procedural safeguards, statutory proportionality, and judicial oversight. Under general criminal doctrine and statutory rules governing the judicial police, investigative powers are strictly auxiliary and subordinate to the Public Prosecution.

In the Jordanian legal system, while judicial police officers are tasked with detecting offenses and gathering evidence under Article 8 of the Criminal Procedure Law, substantive investigative acts remain the exclusive prerogative of the Public Prosecutor, who may only delegate specific tasks to judicial police officers through formal written instructions pursuant to Article 48 of the Law.[288] Consequently, investigative measures must remain strictly confined to the officer's defined statutory competence, be fully documented, and remain subject to direct prosecutorial supervision.

Under established criminal procedure principles, non-consensual searches and inspections of private premises may only be conducted pursuant to prior judicial authorization or prosecutorial warrant; any inspection executed in the absence of such prior legal authorization is rendered legally invalid. These procedural requirements ensure that state investigative measures remain authorized, proportionate, and strictly compliant with due process standards.

This judicial procedural guarantee is explicitly affirmed in parallel domestic legislation, such as the Jordanian Electronic Crimes Law, which stipulates that, subject to applicable legal provisions and the personal rights of the defendant, judicial police officials may enter and search premises where evidence indicates the commission of an offense only after obtaining formal prior permission from the competent Public Prosecutor or court. They are likewise authorized to examine digital devices, software applications, operating systems, and information networks, provided they submit a comprehensive inspection report to the judicial authority.[289]

[287] Ibid., Article 13(a).
[288] Jordan, Criminal Procedures Law and its Amendments No. 9 of 1961, Articles (8,48).
[289] Jordan, Electronic Crimes Law No. 17 of 2023, Article 32(A).

In sharp contrast, Article 13 of the Jordanian Cybersecurity Law does not mandate prior prosecutorial authorization for NCSC officials exercising judicial police authority. This statutory omission creates a direct conflict with recognized human rights benchmarks, private property guarantees, and constitutional fair trial protections, highlighting an urgent need for statutory alignment with established criminal procedural safeguards.

IV.1.1.4 Enforcement Mechanisms, Oversight, and Sanctions

IV.1.1.4.1 Regulatory Compliance and Mandatory Cooperation

The Jordanian Cybersecurity Law authorizes the NCSC to receive "complaints and reports relevant to cybersecurity and cybersecurity incidents" and grants it the discretion to follow up and take appropriate measures. From a strict legal taxonomy perspective, this statutory formulation is imprecise. What the law effectively regulates is not cybersecurity complaints themselves, but rather the mandatory notification of such incidents to the competent administrative authority. Accordingly, the provision should more accurately refer to cybersecurity incident notifications.

The statute appears to equate complaints with incident notifications within this context; however, these two concepts are fundamentally distinct in legal nature and procedural effect. Complaints are inherently linked to judicial procedures and the formal initiation of criminal prosecution before prosecutorial or judicial authorities. A complaint presupposes a bilateral legal dispute initiated by an affected victim against a specific, identifiable perpetrator.[290]

By contrast, incident notifications function as preventive administrative mechanisms aimed at enabling early threat detection, rapid containment, and the mitigation of operational vulnerabilities.[291] An incident notification may be submitted by any party aware of a threat or breach, even where the threat actor remains completely anonymous or passive.

Therefore, while empowering the NCSC to receive cybersecurity incident notifications is consistent with its preventive, regulatory, and coordination mandate, the designation of the Center as the competent authority to receive complaints reveals a conceptual and regulatory gap. Such designation is inconsistent with the Center's institutional role and does not conform to the judicial

[290] NAMOUR, 2024, p.198.

[291] See Cybersecurity incident definition under the Jordanian's Cybersecurity Law No.16 for 2019, Article 2.

procedures governing the initiation of criminal proceedings under Jordanian criminal procedure law.

Furthermore, the statutory reference to reports relevant to cybersecurity is formulated in broad and vague terms, lacking a precise legal definition and extending beyond the scope of incident-based reporting addressed elsewhere in the statute. Most critically, the provision states that the Center may follow up on such complaints and reports, thereby framing administrative enforcement as discretionary rather than obligatory.

Given the Center's role as the national authority responsible for cybersecurity governance, this permissive formulation appears inconsistent with the preventive and protective objectives of the law. Effective cybersecurity governance requires mandatory response and follow-up mechanisms, particularly in relation to incidents that may threaten national security or critical infrastructure. Accordingly, the discretionary language employed in Article 8(A) of the Law risks undermining enforcement efficacy and weakening legal certainty. This internal inconsistency becomes more apparent when Article 8(A) is examined in conjunction with Article 8(B) of the same Law.

To this extent, Article 8(B) establishes clear and binding statutory duties for ministries, governmental departments, public bodies, and private entities. These duties include full compliance with the Center's technical policies, standards, and sector-specific security conditions, providing the Center with operational information necessary to execute its supervisory functions, and the mandatory reporting of cybersecurity incidents alongside the execution of preventive controls. [292]

Legally, these obligations create a mandatory statutory compliance framework, reinforcing the Center's coordinating and *ex-ante* role. Unlike the permissive language of Article 8(A), Article 8(B) aligns with fundamental administrative principles, ensuring that regulated entities contribute to systemic monitoring, threat reporting, and operational risk mitigation.

IV.1.1.4.2. Cybersecurity Incident Management

Cybersecurity incident management is the systematic process of identifying, managing, documenting, and analyzing security threats and cyber-related risks in real-world contexts. This

[292] Jordan, Cybersecurity Law No. 16 of 2019, Article 8(b).

process is a critical step, whether implemented proactively before a cyber disaster occurs or reactively afterward, within an entity's IT infrastructure.[293] Effective incident management relies on technical expertise and operational readiness, enabling regulated actors to minimize damage and prevent localized vulnerabilities from escalating into systemic failures.

From a legal governance perspective, Jordan's regulatory framework must balance operational flexibility with the rule of law, particularly where incident responses entail binding compliance orders or state intervention. A core component of this balance is a transparent incident classification scheme, which provides the legal and operational justification for prioritizing responses and determining the degree of administrative intervention.

Within the Jordanian legal framework, cybersecurity incident management is primarily regulated through Article 9 of the Cybersecurity Law and the Cybersecurity Incident Classification Instructions of 2023,[294] which were issued pursuant to the Law. Together, these instruments seek to establish a centralized and coordinated response mechanism for cybersecurity incidents, especially those of heightened national significance.

Article 9(A) of the Cybersecurity Law authorizes the National Cybersecurity Council, upon the recommendation of the Chief Officer of the NCSC, to determine whether a cybersecurity incident represents a threat to the security and integrity of the Kingdom.[295] Correspondingly, Article 8 of the 2023 Instructions provides that, where an incident constitutes such a threat, the Center shall assume responsibility for managing and directing the response, and all concerned entities are legally bound to comply with its instructions. This alignment reflects a clear legislative intent to centralize decision-making and operational control in cases involving national cybersecurity risks.[296]

---

[293] GeeksforGeeks, Incident Management in Cyber Security, available at: https://www.geeksforgeeks.org/computer-networks/incident-management-in-cyber-security/ (Accessed 24 January 2026).
[294] Jordan, Instructions for the Classification of Cybersecurity Incidents for the Year 2023, issued pursuant to Clause (3) of Paragraph (b) of Article 6 of the Cybersecurity Law No. 16 of 2019, 2023, available at: https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/cyber_security_incidents_categorization_instructions_2023.pdf, (Accessed on 25 January 2026).
[295] Jordan, Cybersecurity Law No. 16 of 2019, Article 9(A).
[296] Jordan, Instructions for the Classification of Cybersecurity Incidents for the Year 2023, issued pursuant to Clause (3) of Paragraph (b) of Article 6 of the Cybersecurity Law No. 16 of 2019, 2023, Article (8). available at: https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/cyber_security_incidents_categorization_instructions_2023.pdf, (Accessed on 25 January 2026).

The Instructions further elaborate on this framework by introducing a structured, risk-based classification system that categorizes cybersecurity incidents into four levels—severe, serious, medium, and low—based on objective indicators such as service disruption, data compromise, affected sectors, and population impact.[297] This classification mechanism serves an important regulatory function by promoting predictability, proportionality, and consistency in incident response. However, despite this detailed framework, both the Law and the Instructions establish an overriding, unclassified category for incidents that represent a "threat to the security and integrity of the Kingdom". This category operates independently of the standard four-tier classification system and is not governed by objective statutory criteria. Neither Article 9 of the Law nor Article 8 of the Instructions specifies the quantitative thresholds or substantive standards required to justify such a designation, nor do they clarify its legal relationship to the highest-risk category of "severe" incidents.

This regulatory gap creates significant legal uncertainty. Decisions adopted under Article 9 are inherently more consequential than those associated with even the most severe classified incidents, as they trigger centralized national control and impose mandatory compliance obligations across all sectors. Yet, in the absence of statutory standards, determining what constitutes a threat to national security is left to discretionary decision by the Council. This creates uncertainty as to the legal justification of such decisions and opens the possibility that any cybersecurity incident, regardless of its objective severity, could be elevated to this exceptional category by decision of the Council alone.

Article 9 (B) outlines the operational role of the NCSC in responding to incidents identified under Article 9(A).[298] While the Council determines whether an incident constitutes a threat to the security and integrity of the Kingdom, the Center is tasked with managing the response and issuing instructions that all relevant entities must follow. When considered alongside Articles (3,4) of the Law the National Cybersecurity Center Regulation,[299] these provisions reflect the statutory division between the Council's strategic policy functions and the Center's executive governance role.

[297] Ibid., Articles (3,4,5,6,7).
[298] Jordan, Cybersecurity Law No. 16 of 2019, Article 9(A, B).
[299] Jordan, National Cybersecurity Center Regulation No. 1 of 2020, Articles (3,4).

IV.1.1.4.3 Licensing, Delegation, and Oversight of Cybersecurity Service Providers

Unlike the EU NIS2 Directive, which does not establish a single, general category of "cybersecurity service providers" but instead identifies and regulates specific categories of service providers, including managed service providers (MSPs) and MSSPs, the Jordanian Cybersecurity Law No. 16 of 2019 expressly defines "Cybersecurity Services" as technical, administrative, and advisory activities in the field of cybersecurity, including security assessment, monitoring, auditing, and advisory services.[300] The Law also provides for the licensing of cybersecurity service providers, thereby establishing a distinct regulatory category for entities providing such services.

The Law establishes a formal licensing framework, vesting the NCSC with statutory authority to grant licenses subject to specific technical, administrative, and financial qualifications.[301] Article 10 prohibits any entity from offering commercial cybersecurity services without prior authorization, requiring existing vendors to regularize their legal status.[302] Additionally, Article 11 permits the Center to delegate specific supervisory duties to other public or regulatory bodies while maintaining centralized reporting oversight.[303]

Complementing this statutory framework, the Cybersecurity Service Providers Regulation was enacted in 2024 pursuant to the Cybersecurity Law; it elaborates the operational duties of licensed providers. Service providers are expected to deliver services in accordance with established standards and qualifications, furnish the Center with necessary documentation for regulatory oversight, and maintain strict confidentiality over client information.[304]

In addition, they must retain records of services rendered for a defined period and maintain detailed registers of service recipients and personnel, which remain subject to review by the Center.[305] Collectively, these requirements reflect a regulatory approach that transcends simple licensing, promoting compliance, transparency, and alignment with national cybersecurity governance objectives.

[300] Jordan, Cybersecurity Law No. 16 of 2019, Article 2.
[301] Jordan, Cybersecurity Law No. 16 of 2019, Article 6 (B)(4).
[302] Ibid., Article 10.
[303] Ibid., Article 11.
[304] Jordan, Cybersecurity Service Providers Licensing Regulation No. 76 of 2024, Article 9.
[305] Ibid.

However, this regulatory model remains predominantly reactive, focusing heavily on incident reporting after a breach occurs rather than mandating *ex-ante* risk provision. A notable weakness lies in the absence of a clear distinction regarding the level or severity of incidents that must be reported. Minor incidents, which may have negligible impact on individuals or organizations, are treated equivalently to more severe incidents, creating potential inefficiencies and regulatory ambiguity.[306]

Furthermore, neither the Law nor its implementing regulations explicitly require licensed service providers to implement continuous internal risk management frameworks. This omission limits the incentive for vendors to adopt forward-looking security management beyond basic statutory compliance and reflects a regulatory framework that remains predominantly compliance-oriented rather than risk-oriented. As a result, the existing framework places greater emphasis on post-incident obligations than on continuous preventive risk management and organizational resilience.

IV.1.1.4.4 Administrative Sanctions and Legal Accountability

The Jordanian Cybersecurity Law adopts a comprehensive enforcement model that combines administrative and punitive sanctions in order to ensure compliance with cybersecurity obligations. Article 16 of the Law, supplemented by the Instructions for Determining the Standards of Cyber Security Law Violations for 2025,[307] establishes a graduated sanctions regime that reflects the regulatory nature of most cybersecurity infringements. This framework is designed to respond proportionately to violations based on their severity, recurrence, and the legal status of the violating entity.

To this extent, the core of the sanction's regime consists of administrative measures aimed at restoring compliance and preventing future violations. Article 16(A) empowers the NCSC to impose one or more non-penal measures, including written warnings, orders to rectify violations within a specified period, and the recovery of expenses incurred by the Center as a result of the breach. These measures reflect a regulatory approach that prioritizes remediation over punishment,

[306] Jordan, Instructions for the Classification of Cybersecurity Incidents for the Year 2023, issued pursuant to Clause (3) of Paragraph (b) of Article 6 of the Cybersecurity Law No. 16 of 2019, 2023, Article 7. available at: https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/cyber_security_incidents_categorization_instructions_2023.pdf, (Accessed on 25 January 2026).

[307] Jordan, Instructions for Determining the Criteria for Violations of the Provisions of the Cybersecurity Law, Their Controls and the Procedures Due Thereto for the Year 2025.

particularly in cases where the violation does not immediately endanger national security or critical infrastructure.

The Instructions further operationalize this approach by establishing procedural safeguards and escalation mechanisms. Violations are documented through formal inspection reports, followed by notification and an opportunity for rectification. The President of the Center may grant extensions where justified, reinforcing the administrative and compliance-oriented character of the system. More intrusive measures such as suspending or canceling licenses, compelling entities to take internal disciplinary action, or restricting access to information systems are reserved for more serious or repeated violations, or for breaches committed by licensed cybersecurity service providers who are subject to heightened professional obligations.

Importantly, the Instructions classify violations based on both the nature of the breach and the status of the violator (licensed, unlicensed, or unauthorized), thereby introducing a differentiated regulatory response. This reflects an implicit recognition that cybersecurity obligations vary according to an entity's role, capacity, and level of responsibility within the cybersecurity ecosystem.[308]

In addition to administrative measures, the Law authorizes the imposition of financial penalties as a deterrent mechanism. Article 16(A)(6) establishes a broad range of fines from 500 to 100,000 JOD allowing the Center to calibrate penalties in proportion to the seriousness of the violation and its potential or actual harm.[309] The Instructions further refine this framework by linking fines to specific categories of violations, such as failure to report incidents, non-compliance with center-issued standards, unauthorized provision of cybersecurity services, or obstruction of enforcement activities.[310]

A notable feature of the system is the escalation of fines in cases involving classified cybersecurity incidents. Where a violation results in, or is suspected of contributing to, a cybersecurity incident, fines are determined according to the incident's severity ranging from moderate to high-risk incidents with corresponding financial penalties reaching up to 100,000

[308] Ibid., Article 5.
[309] Jordan, Cybersecurity Law No. 16 of 2019, Article (16)(A)(6).
[310] Jordan, Instructions for Determining the Criteria for Violations of the Provisions of the Cybersecurity Law, Their Controls and the Procedures Due Thereto for the Year 2025, Article 6.

JOD. Repeated violations trigger mandatory doubling of fines, reinforcing the deterrent function of the sanction's regime.

Despite the graduated structure of this enforcement framework, a critical legal concern arises regarding the administrative treatment of multiple simultaneous violations. Article 5(D) of the 2025 Instructions provides that "in case of multiple violations, the most severe action shall be taken against the violator". This rule empowers the NCSC to consolidate multiple breaches and apply a single penalty. This administrative approach departs from general principles of sanction aggregation under Jordanian Criminal Law, where combining penalties, applying the most severe sanction, or assessing offense concurrence falls within the exclusive jurisdiction of the judiciary.[311]

In judicial practice, when a court elects to apply only the most severe penalty among multiple offenses, such a decision is made after assessing a range of judicial factors, including the degree of fault, causal contribution, proportionality, and the individual circumstances of each offense. By contrast, the Instructions confer upon an administrative authority the power to apply a single sanction for multiple violations without reference to comparable safeguards or evaluative criteria, thereby encroaching upon functions traditionally reserved for the judiciary.

For instance, the North Amman Magistrate Court (Criminal), in Decision No. 6558/2018, opted to combine the penalties rather than apply the most severe one. In its reasoning, the court relied on Article 72 of the Criminal Law, emphasizing that it possesses discretionary authority to choose between combining the penalties or enforcing the harsher punishment. The court explicitly justified its choice by stating that considerations of justice required the aggregation of penalties, particularly in light of the gravity and reprehensible nature of the defendants' acts, which warranted a stricter judicial stance. This decision clearly demonstrates that when Jordanian courts choose to combine punishments, they are required to provide a reasoned justification for exercising this discretion.[312]

Similarly, another court provided explicit justification when choosing to apply the most severe punishment. The Irbid Magistrate Court, in Decision No. 6259/2022, relied on Articles 100 and 72 of the Criminal Law. The court explained that, pursuant to Article 100, and in light of its

[311] Jordan, Criminal Law No. 16 of 1960, Article 72.
[312] Jordan, North Amman Magistrate Court (Criminal), Decision No. 6558/2018, Judgment of 15 June 2018.

discretionary authority to assess mitigating circumstances—particularly the complainant's waiver of the personal right—the reduction of the enforceable penalty was warranted. However, pursuant to Article 72 of the Criminal Law, the court ultimately decided to enforce the most severe punishment against the defendant, determining the applicable penalty accordingly.[313]

The risk arising from violations of cybersecurity provisions is particularly serious, especially where the cybersecurity incident is classified as high-risk. In such cases, the application of the most severe sanction alone, as prescribed under Article 4 of the Instructions, may not fully reflect the legal significance of multiple concurrent violations.

Unlike the approach adopted under certain areas of Jordanian criminal legislation, such as the Economic Crimes Law, which treats each offense independently for the purpose of determining liability, the Cybersecurity Law consolidates multiple violations into a single sanction based on the most serious infringement.[314] This distinction may reduce the proportional relationship between the number of violations committed and the corresponding legal consequences.

This approach has already been embraced by the Jordanian criminal system in special criminal statutes, such as the Economic Crimes Law, which governs offenses against public funds. Article 4/C of that Law expressly provides that penalties shall not be merged where multiple crimes are committed by the same person under its provisions.[315] Accordingly, the Economic Crimes Law adopts the principle of concurrence of penalties (cumulative punishment) rather than penalty merger. This principle requires that a separate sanction be imposed for each offense when multiple crimes occur, thereby ensuring a stricter and more proportionate response to serious violations.

However, more critically, the administrative choice to impose only one sanction for several distinct violations carries significant procedural risks. If the Center selects the most severe measure and that decision is subsequently challenged before the competent court, a judicial finding of non-liability or annulment in respect of that single violation may result in the complete absence of sanctions, notwithstanding the existence of other proven breaches. In effect, the administrative consolidation of multiple violations into a single sanction may inadvertently shield repeat or multi-

[313] Jordan, Irbid Magistrate Court (Criminal), Decision No. 6259/2022, Judgment of 8 May 2023.
[314] Jordan, Instructions for Determining the Criteria for Violations of the Provisions of the Cybersecurity Law, Their Controls and the Procedures Due Thereto for the Year 2025, Article 5(d).
[315] Jordan, Economic Crimes Law No. 11 of 1993, Article 4(c).

faceted offenders from accountability, undermining both the deterrent purpose of the sanction's regime and the principle of individual responsibility for each unlawful act.

Beyond procedural risks in handling multiple violations, a more fundamental constitutional issue concerns the legal nature of the penalties the NCSC is authorized to impose directly under Article 16(A)(6) of the Cybersecurity Law and Article 6 of the 2025 Instructions. Although these provisions formally characterize the sanctions as administrative, the magnitude and effect of the prescribed financial penalties reveal a distinctly criminal character. Under established Jordanian criminal law principles, any fine exceeding thirty Jordanian Dinars constitutes a misdemeanor penalty rather than a disciplinary or administrative measure. Such penalties, by their very nature, fall within the exclusive jurisdiction of the judiciary and may only be imposed following the formal determination of criminal liability through constitutional due process.

This statutory arrangement conflicts directly with Article 102 of the Jordanian Constitution, which guarantees that judicial power and the administration of justice reside exclusively within courts established by law.[316] By empowering an executive administrative body to directly issue fines reaching up to 100,000 JOD, the law creates an unconstitutional delegation of judicial authority to the executive branch, circumventing the exclusive jurisdiction of the judiciary and the procedural due process required for determining criminal liability.

This distinction is not merely terminological, but reflects a foundational principle of criminal legality: *nullum crimen, nulla poena sine judice*, which requires that no criminal sanction be imposed without judicial adjudication.[317] Administrative and disciplinary sanctions may lawfully be applied by governmental authorities in the exercise of regulatory oversight.

Notwithstanding this, the Cybersecurity Law and the Instructions designate the NCSC as the competent authority to impose these penalties directly. This legislative choice represents a departure from general Jordanian criminal law principles, which reserve the power to impose criminal sanctions exclusively to courts.

Amman Court of First Instance in its appellate capacity confirmed this principle in Decision No. 6267/2018, stating "No penal measure may be taken against any person except in accordance

[316] Jordan, The Constitution of the Hashemite Kingdom of Jordan of 1952, Article 102.
[317] Jordan, Criminal Law No. 16 of 1960, Article 3.

with the law and under judicial supervision".[318] Since no penalty may be imposed on any person except by virtue of a judicial judgment, this necessarily means that no judicial ruling may be issued unless a criminal case is brought against the accused, who is presumed innocent until proven guilty through legally valid evidence obtained in accordance with the provisions of the law.

This legislative approach departs from the traditional separation between administrative regulation and criminal adjudication. By conferring punitive powers on a specialized administrative authority, the statutory framework raises questions concerning its compatibility with established principles of criminal justice, judicial competence, and constitutional due process.

It could be argued that responding to cyber threats requires swift, specialized intervention; therefore, the NCSC must be empowered to impose direct penalties.[319] However, administrative convenience alone cannot displace fundamental judicial safeguards. The direct imposition of punitive sanctions by an administrative authority raises concerns regarding compliance with the principles of due process, judicial oversight, and the right to a hearing before an independent tribunal. At the same time, this concern relates only to sanctions possessing a criminal character and does not affect the center's broader regulatory and administrative enforcement powers under Article 16 of the Cybersecurity Law.

This finding is further supported by the legal status accorded to the Center's officials. While Article 13 of the Cybersecurity Law[320] and Article 3(C) of the Instructions[321] grant designated officials the authority to document violations and prepare reports, such powers must consistent with the functions of judicial police officers as regulated under Article 100 of the Jordanian Criminal Procedure Law.[322]

These powers are inherently investigative and evidentiary in nature, enabling the detection and documentation of violations, but do not extend to adjudication or punishment. Consequently, empowering the NCSC to impose misdemeanor-level penalties exceeds the permissible bounds of

[318] Jordan, Amman Court of First Instance (Criminal Division, Appellate Jurisdiction), Decision No. 6267/2018, Judgment of 8 November 2018.
[319] BUSETTI – SCANNI, 2024, p.2.
[320] Jordan, Cybersecurity Law No. 16 of 2019, Article 13.
[321] Jordan, Instructions for Determining the Criteria for Violations of the Provisions of the Cybersecurity Law, Their Controls and the Procedures Due Thereto for the Year 2025, Article 3(C).
[322] Jordan, Criminal Procedures Law and its Amendments No. 9 of 1961, Article 100.

administrative enforcement and effectively conflates investigative, regulatory, and punitive functions within a single authority.

Accordingly, the current sanctioning framework raises serious concerns regarding the erosion of judicial oversight, the dilution of procedural guarantees, and the circumvention of the principle of legality. By authorizing an administrative body to impose sanctions of a criminal nature, the Cybersecurity Law risks undermining the procedural safeguards that underpin Jordanian criminal justice, thereby calling into question the conformity of this framework with fundamental principles of criminal law and due process.

IV.2 Complementary Cybersecurity Legislation

IV.2.1 Jordan's Personal Data Protection Law (PDPL)

The concept of personal data protection in Jordan only gained formal legal recognition with the enactment of the PDPL No. 24 of 2023.[323] This landmark statute introduced, for the first time, a dedicated and comprehensive model for safeguarding personal data. Prior to its enactment, data privacy remained largely unregulated in primary legislation, with only limited provisions under former Electronic Crimes Law No. 17 of 2023 addressing narrow issues such as unauthorized data access, alteration, deletion, or disclosure.[324]

The Jordanian PDPL No. 24 of 2023 entered into force on 17 March 2024, accompanied by a one-year transitional period to allow relevant public and private entities to achieve compliance. This grace period enabled organizations to adapt internal processing workflows, upgrade technical security architectures, and revise privacy policies to align with statutory requirements. Its enactment marks a major development in Jordan's data governance landscape, elevating public trust and reinforcing investor confidence in the national digital economy.

The legislation establishes a comprehensive regulatory architecture governing the collection, processing, storage, and cross-border transfer of personal data. From an administrative cybersecurity governance perspective, these statutory provisions are central to mitigating systemic digital vulnerabilities. The law addresses risk vectors associated with unauthorized access, data exfiltration, and processing misuse by establishing core statutory principles, including data

[323] Jordan, PDPL No. 24 of 2023.
[324] Jordan, Electronic Crimes Law No. 17 of 2023.

minimization, explicit prior consent, processing transparency, and data controller and processor accountability.[325] These principles serve as mandatory benchmarks for evaluating compliance and strengthening the security, integrity, and resilience of data processing infrastructure across both public and private sectors.

Modern digital and data-driven architectures frequently operate with minimal direct user interaction while continuously processing vast volumes of personal and sensitive data. Pursuant to the PDPL, personal data may not be processed without the explicit, informed, and prior consent of the data subject, unless a clearly defined statutory exception applies. This requirement obligates data controllers and processors to implement robust governance and technical controls ensuring that consent is properly obtained, logged, and managed, and that data subjects are fully informed regarding processing purposes, retention periods, technical security safeguards, and third-party data sharing practices.[326]

In alignment with the Cybersecurity Law's emphasis on rapid incident reporting, the PDPL similarly obliges controllers to notify affected data subjects within 24 hours of discovering a serious breach that could cause significant harm, and to report the incident to the regulatory unit within the Ministry of Digital Economy and Entrepreneurship within 72 hours, detailing the breach's source, mechanism, and impacted data.[327] This parallel notification mechanism underscores the complementary relationship between data protection and cybersecurity frameworks, both aimed at embedding proactive risk management, institutional accountability, and operational resilience across Jordan's digital ecosystem.

Building upon these governance duties, the PDPL mandates that data controllers implement necessary technical and organizational measures to protect data integrity and confidentiality. [328] While the primary statute establishes this broad duty, specific controls—such as data encryption, secure storage, system updates, and vulnerability assessments—are operationalized through specialized implementing instructions.

[325] Jordan, PDPL No. 24 of 2023, Articles (5,6,7).
[326] Ibid., Article 4.
[327] Ibid., Article 20.
[328] Ibid., Article 8(b).

The mandatory appointment of a Data Protection Officer (DPO) in the cases specified by Article 11 reinforces this security-oriented approach by assigning responsibility for compliance oversight, data governance, and the implementation of internal security and data-lifecycle policies.[329] In parallel, the law grants data subjects' enforceable rights, including access, rectification, erasure, and withdrawal of consent, which necessitate secure and responsive mechanisms capable of safeguarding data integrity and confidentiality.[330] Non-compliance with these obligations, including failures in breach detection or timely incident notification, may result in significant legal and financial liabilities.

While Jordan has achieved significant legislative progress in data governance through the PDPL, critical regulatory and institutional gaps remain within the emerging framework. A primary challenge stems from limited technical and legal awareness among individuals and SMEs regarding data security mandates. When combined with the rapid pace of organizational digital transformation, this capacity deficit complicates uniform regulatory enforcement across sectors.[331]

A second critical gap concerns the substantive overlap between the PDPL and Cybersecurity Law No. 16 of 2019. In regulatory practice, a cybersecurity incident as defined under Article 2 of the Cybersecurity Law, encompasses not only hardware systems, network infrastructure, and internet platforms, but also digital data itself.[332]

This substantive overlap creates potential jurisdictional and procedural friction between the NCSC and the Ministry of Digital Economy and Entrepreneurship. Without formal inter-agency coordination protocols, regulated entities face dual reporting demands and conflicting administrative instructions during real-time incident responses.

Although the PDPL sets clear statutory benchmarks, its practical execution faces significant institutional constraints. Monitoring compliance across public and private sectors remains difficult for the Personal Data Protection Unit, and verified evidence concerning adherence to technical safeguards like data encryption and vulnerability management is largely lacking.[333]

---

[329] Ibid., Article 11.
[330] Ibid., Articles (4(b), 49).
[331] ALSOBEH et al., 2023, p.15.
[332] Jordan, Cybersecurity Law No. 16 of 2019, Article 2.
[333] Jaradat Law, The Data Protection Council in Jordan and Compliance for International Companies, available at: https://jaradatlaw.com/the-data-protection-council-in-jordan-and-compliance-for-international-

These compliance demands fall heavily on SMEs, whose financial and operational limits often preclude the hiring of specialized DPOs or the deployment of high-cost security infrastructure. This gap between legislative intent and real-world compliance demonstrates that black-letter data protection rules cannot secure digital ecosystems without dedicated regulatory monitoring, targeted compliance support for smaller entities, and expanded state administrative capacity.[334]

IV.2.2 The Electronic Crimes Law

In 2010, Jordan introduced its first Electronic Crime Legislation, the Temporary Information Systems Crime Law No. 30 of 2010, marking a foundational step toward criminalizing digital offenses at the national level.[335] This initial statute focused on offenses committed via electronic platforms, including the distribution of pornographic material, online blackmail, minor sexual exploitation, prostitution promotion, and the deployment of information systems for terrorist activities or incitement to violence.

By 2015, the rapid advancement of information technology and the increasing sophistication of cyber threats prompted the Jordanian legislator to expand the legal framework. The Law on Information Systems Crimes was amended and retitled as the Electronic Crimes Law, incorporating new provisions to address emerging forms of digital misconduct.

These amendments not only criminalized electronic extortion and fraud but also provided legal protection for information systems, networks, and both tangible and intangible assets, commonly referred to as cyber assets. Although a clear separation between cybercrimes and purely electronic crimes could have enhanced the law's clarity, the 2015 amendments succeeded in broadening the substantive scope of offenses targeting information systems and network-related crimes.[336]

Despite these advancements, the 2015 Electronic Crimes Law exhibited notable shortcomings regarding data privacy and technical security governance. Key deficiencies included

companies/#:~:text=Jordan's%20Personal%20Data%20Protection%20Law,regulatory%20unit%20within%20the%20government.&text=Challenges%3A%20New%20compliance%20costs%2C%20stricter,oversight%2C%20potential%20fines%20for%20non-compliance (Accessed 27 Feb. 2026).

[334] RISWALDI, 2025, p.347.

[335] Jordan, Electronic Crimes Law No. 27 of 2015.

[336] Ibid., Articles (3,4).

imprecise definitions, weak guidance on lawful data processing, the absence of explicit consent requirements, limited data subject rights, and unregulated cross-border data transfers, leaving digital systems and individual data assets exposed to misuse.[337] Consequently, the legislature enacted Electronic Crimes Law No. 17 of 2023, expanding the substantive scope of criminalized conduct and escalating penal deterrence.[338]

The 2023 Electronic Crimes Law significantly broadens criminal liability for unauthorized actions affecting data assets and information networks. Articles 3, 4, and 6 cover unauthorized access, manipulation, disruption, or interference with digital infrastructure using any information technology tools.[339] Prohibited acts include deleting, altering, encrypting, exfiltrating, or destroying data, obstructing system operations, and impersonating administrative users.[340]

Compared to the 2015 statute, the 2023 amendments introduced "information technology tools" as an expanded statutory medium for committing cyber offenses. The updated law also significantly increased financial and custodial penalties for unauthorized data manipulation and system disruption under Article 6, prescribing mandatory imprisonment of not less than six months and fines ranging from 2,500 to 10,000 Jordanian Dinars (JOD).[341] By contrast, the corresponding provision under the 2015 law prescribed imprisonment of three months to one year and fines of 200 to 1,000 JOD, reflecting a clear escalation in legal deterrence aimed at confronting modern cyber risks.[342]

Against this background, the distinction between a cybersecurity incident and a cybercrime becomes particularly relevant to the criminal-law framework. Although the Cybersecurity Law recognizes the cybersecurity incident as a legally relevant event requiring a response to prevent or mitigate its consequences,[343] the Electronic Crimes Law did not establish the occurrence of such an incident as an autonomous criminal offence. Nor did it expressly provide for criminal liability merely on the basis of a serious security breach resulting from organizational negligence.

[337] KHWAILEH, 2025, p.2949.
[338] Jordan, Electronic Crimes law No. 17 of 2023.
[339] Ibid., Articles (3,4,6).
[340] Ibid., Article 6.
[341] Ibid.
[342] Jordan, Electronic Crimes Law No. 27 of 2015, Article 4.
[343] Jordan, Cybersecurity Law No. 16 of 2019, Article 2.

Accordingly, the occurrence of a cybersecurity incident does not, in itself, establish criminal liability. Criminal liability under the former Electronic Crimes Law depends instead on whether the conduct underlying the incident fulfils the constituent elements of a specifically defined electronic crime, including the requisite mental element where required. Thus, an incident may have significant consequences from a cybersecurity-governance perspective without necessarily constituting a criminal offence.[344]

However, pursuant to Article 2 of the Cybersecurity Law, an incident is formally characterized as an "attack".[345] Although an attack may involve deliberate conduct by a threat actor and may therefore provide the factual basis for criminal liability, its characterization as an “attack” under the Cybersecurity Law does not, by itself, establish the mental element (*mens rea*) required for a particular criminal offence.[346] The existence of criminal liability must instead be determined by reference to the specific statutory elements of the applicable offence, including the required form of culpability.

Moreover, even where a cybersecurity incident arises from human error, criminal liability may still be engaged where the applicable criminal provision recognizes negligence as a sufficient basis for liability and where the conduct satisfies all other elements of the offence. According to current Electronic Crimes law rules, negligence cannot automatically be treated as the mental element of an electronic offence merely because a cybersecurity incident resulted from human error, lack of due care, or non-compliance with applicable laws and regulations. While general criminal law may recognize liability for certain unintentional offences, such as unintentional bodily harm, this does not by itself establish criminal liability for cybersecurity incidents or electronic offences under the current Law.[347]

Consequently, the more significant legislative question is not whether cybersecurity incidents as such should be criminalized, but whether the existing electronic-crimes framework provides an adequate basis for addressing serious and culpable failures to comply with legally mandated cybersecurity obligations. Where a serious cybersecurity incident results from gross or

[344] MOURAD, 2025, p.39.
[345] Jordan, Cybersecurity Law No. 16 of 2019, Article 2.
[346] SINROD – REILLY, 2000, p.30.
[347] Jordan, Criminal Law No. 16 of 1960, Article 334.

reckless organizational failure and the underlying conduct does not fall within an existing criminal offence, the absence of a specific criminal-law mechanism may create an accountability gap.

Chapter V: A Critical Comparative Assessment of Cybersecurity Governance in the EU and Jordan

V.1 Comparative Framework for Assessment

Building on the preceding analysis of the cybersecurity legal frameworks in Jordan and the EU, this chapter undertakes a critical comparative assessment of the key legal principles that underpin cybersecurity governance in both jurisdictions. While Chapter IV examined Jordan's domestic cybersecurity legislation, institutional architecture, enforcement mechanisms, and complementary legal regimes, this chapter moves from doctrinal description to functional comparative analysis.

The comparison is structured around four interconnected phases of cybersecurity governance: preventive measures, reactive responses, post-incident mechanisms, and lifecycle security.[348] It does not seek to establish an abstract hierarchy between the EU and Jordanian systems or to treat the EU framework as a model for automatic transplantation. Rather, it examines how each legal order addresses common cybersecurity challenges and whether differences in legislative design, institutional competence, risk allocation, and enforcement produce materially different regulatory outcomes.

Accordingly, the analysis focuses on four questions: what legal and institutional mechanisms have been established; how those mechanisms operate and what obligations or powers they generate; what structural divergences exist between the two frameworks; and what consequences those divergences have for cybersecurity resilience. This approach distinguishes differences in legislative technique from divergences that materially affect regulatory effectiveness.

Consequently, the EU framework is not evaluated as an idealized model to be uncritically transplanted into Jordan. Its regulatory mechanisms are assessed alongside their institutional, economic, and market implications. Where the EU framework demonstrates greater regulatory integration, the analysis considers the institutional and economic conditions supporting that

[348] VALKENBURG – BONGIOVANNI, 2024, p.2.

integration. Conversely, potential compliance costs, administrative complexity, and implementation burdens, particularly for SMEs, are also taken into account.

The chapter therefore remains diagnostic rather than prescriptive. It identifies structural convergence and divergence, institutional capacity gaps, and regulatory friction, while specific legislative amendments, institutional restructuring, and policy recommendations are reserved for the subsequent reform roadmap.

V.2 Operationalizing the Regulatory Maturity Matrix

V.2.1 Analytical Dimensions and Maturity Tiers

To move beyond descriptive instrument-by-instrument comparison, this chapter operationalizes a structured analytical tool designated as the Regulatory Maturity Matrix. Rather than evaluating statutory texts in isolation, the Matrix provides a consistent framework for assessing the regulatory maturity of each jurisdiction and examining its implications for regulatory effectiveness and systemic resilience.

For analytical consistency, each dimension is assessed against three maturity tiers. High maturity reflects precise and enforceable statutory duties, differentiated and risk-calibrated obligations, effective supervisory institutions, meaningful accountability mechanisms, and operational coordination. Medium maturity reflects a formal legal framework whose effectiveness is constrained by broad administrative discretion, limited risk differentiation, developing verification mechanisms, or institutional concentration. Nascent or low maturity reflects substantial reliance on non-binding guidance, voluntary compliance, fragmented institutional authority, or limited enforceability.

The first dimension, legal bindingness, examines the statutory weight and normative specificity of the applicable legal instruments. The EU framework operates through a highly codified legal hierarchy dominated by directly applicable instruments, such as the GDPR and the CRA, alongside deeply harmonized frameworks like the NIS2 Directive that require national implementation.

This combination provides substantial normative precision and, particularly in the case of regulations, direct applicability, while NIS2 establishes harmonized obligations through national transposition. Conversely, the Jordanian framework relies on the primary framework statute,

Cybersecurity Law No. 16 of 2019, which delegates significant regulatory detail to secondary legislation, instructions, and administrative instruments. While this structure may provide administrative flexibility, it also raises questions concerning the precision, hierarchy, and enforceability of subordinate regulatory requirements.

The second dimension, risk proportionality, examines how cybersecurity obligations are calibrated according to the level and nature of risk. The EU framework more explicitly differentiates regulatory obligations according to factors such as entity type, sectoral significance, risk exposure, and the nature of the regulated activity, particularly under NIS2 and the GDPR. In contrast, the Jordanian framework has comparatively less developed statutory mechanisms for differentiating cybersecurity obligations according to organizational risk, sectoral criticality, or entity characteristics.

The third dimension, enforcement mechanisms, evaluates the extent to which regulatory duties are supported by effective supervisory and accountability mechanisms. The EU combines national competent authorities, supervisory bodies, market-surveillance mechanisms, administrative sanctions, and judicial review across different regulatory instruments. Jordan, by contrast, relies more heavily on centralized administrative enforcement through the national cybersecurity architecture, with comparatively less differentiated supervisory structures across sectors.

The fourth dimension, institutional capacity, evaluates the distribution and specialization of regulatory authority. The EU utilizes a multi-level governance structure involving national competent authorities, CSIRTs, ENISA, and EU-CyCLONe, thereby distributing cybersecurity responsibilities across national and Union levels. Jordan, by contrast, relies on a more centralized institutional architecture centered on the NCSC. While centralization may facilitate coordinated national responses, it may also place greater institutional demands on a relatively concentrated governance structure.

The fifth dimension, private-sector engagement, examines the extent to which non-state actors are integrated into cybersecurity governance. The EU framework assigns significant regulatory responsibilities to regulated entities, digital service providers, MSPs, MSSPs, and, under the CRA, manufacturers and other economic operators involved in the digital product lifecycle. Jordan, by contrast, has developed mechanisms for regulating and licensing

cybersecurity service providers, but the integration of private-sector actors into the broader cybersecurity governance architecture remains comparatively less developed.

Lifecycle continuity concerns whether legal obligations extend beyond initial compliance or incident response to continuous vulnerability management, security maintenance, and product or service lifecycle responsibilities. The EU framework demonstrates greater regulatory continuity, particularly through the CRA's lifecycle-oriented obligations and NIS2's risk-management and incident-related requirements. Jordan's framework remains comparatively more focused on organizational cybersecurity obligations and incident response, with less extensive statutory regulation of cybersecurity across the full technological lifecycle.

Resilience integration examines whether the legal framework connects prevention, preparedness, response, recovery, and learning into a continuous governance cycle. While the EU framework increasingly integrates these functions across multiple instruments, Jordan's framework remains comparatively more concentrated on prevention, incident response, and executive coordination, with less developed statutory mechanisms for systematic post-incident verification and institutional learning.

Operational interoperability evaluates the capacity of legal and institutional structures to facilitate coordinated action and information exchange across sectors and jurisdictions. The EU framework provides more extensive mechanisms for cross-border cooperation and structured cybersecurity information exchange. Jordan's framework, although increasingly oriented toward national coordination, provides comparatively less developed mechanisms for systematic cross-sectoral and international interoperability.

V.2.2 Application of the Matrix to Thematic Areas

The Regulatory Maturity Matrix provides the analytical framework through which the subsequent thematic areas are comparatively assessed. Rather than evaluating cybersecurity regulation solely through isolated legal provisions, the Matrix is applied across the four governance phases identified above in order to identify broader structural patterns and regulatory divergences between the EU and Jordan.

Preventive mechanisms in Section V.3 are assessed primarily through legal bindingness, risk proportionality, institutional capacity, and private-sector engagement. Reactive mechanisms

in Section V.4 are examined through enforcement mechanisms, institutional coordination, and operational interoperability, particularly in relation to incident reporting and breach notification.

Post-incident mechanisms in Section V.5 are assessed primarily through resilience integration, enforcement, and institutional accountability, while lifecycle mechanisms in Section V.6 are examined through lifecycle continuity, private-sector engagement, and operational interoperability. The Matrix therefore provides a common analytical basis for evaluating not merely the formal existence of statutory provisions, but the extent to which each legal system achieves enforceability, institutional coordination, risk responsiveness, and continuous cybersecurity resilience.

V.3 Preventative Cybersecurity Mechanisms

Preventative mechanisms constitute the first line of defense in cybersecurity governance, aiming to reduce vulnerabilities and mitigate risks before security incidents occur.[349] Within both the EU and Jordanian frameworks, such mechanisms are primarily reflected in digital certification schemes, risk management obligations, and data processing security standards. However, their legislative design and level of regulatory maturity differ significantly, reflecting broader structural divergences identified in the Regulatory Maturity Matrix, particularly regarding legal bindingness, institutional capacity, risk proportionality, and lifecycle continuity.

V.3.1 Digital Product Certification and Conformity Assessment

The strengthening of preventive cybersecurity governance increasingly relies on certification and conformity assessment mechanisms designed to ensure that digital products and services satisfy defined cybersecurity requirements prior to market deployment.[350] Within the EU, preventative regulation combines distinct legal instruments: the CSA establishes the European cybersecurity certification framework—which is generally voluntary unless otherwise mandated—while the CRA imposes binding substantive cybersecurity requirements across the product lifecycle.[351] Together, they mark a shift toward mandatory, lifecycle-integrated product security.

---

[349] Swanagan, Michael, The 3 Types of Security Controls (Expert Explains). PurpleSec, 6 October 2025. Available at: https://purplesec.us/learn/security-controls/ (Accessed: 14 August 2026).

[350] KHURSHID et al., 2022, p.129939.

[351] European Parliament and Council of the European Union, Regulation (EU) 2019/881 (Cybersecurity Act); and Regulation (EU) 2024/2847 (Cyber Resilience Act), Articles 24 and 32 (governing conformity assessment procedures).

From a preventative governance perspective, certification mechanisms serve multiple regulatory functions: establishing baseline cybersecurity requirements, promoting trust within digital markets, encouraging secure-by-design practices, and facilitating regulatory coordination across supply chains.[352] Furthermore, recent EU cybersecurity regulation increasingly extends cybersecurity obligations beyond initial market placement to include ongoing vulnerability management, monitoring, and product support responsibilities.

Nevertheless, the practical operation of certification mechanisms within the EU reveals important structural complexities. Existing certification schemes do not always sufficiently differentiate between varying technological contexts, operational environments, and sector-specific risk profiles. This creates an inherent tension between regulatory standardization and technological diversity, potentially limiting the precision and adaptability of certification frameworks across different categories of digital products.

These complexities have become more pronounced following the introduction of the CRA. While the Regulation strengthens legal bindingness and enhances enforceability through mandatory cybersecurity obligations applicable to products with digital elements, it also introduces uncertainty regarding product classification and the interaction between overlapping regulatory instruments.

In particular, the relationship between the CRA and the NIS2 Directive may generate ambiguity concerning the applicable level of cybersecurity obligations, as these frameworks utilize different regulatory coordinates: the CRA classifies products horizontally based on their technical characteristics and intended functionalities, [353] whereas NIS2 determines entity obligations based on the sectoral status and operational criticality of end users.[354] Consequently, a digital product subject to baseline CRA requirements may be deployed within critical infrastructure environments governed by stringent NIS2 mandates, creating complex shared responsibility and compliance interfaces between manufacturers and essential or important entities.

[352] TEICHMANN, 2026, p.11.
[353] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), Articles (6,7).
[354] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Articles (3,21).

Measured against the evaluative criteria of the Regulatory Maturity Matrix, the EU framework demonstrates a high degree of legal bindingness, institutional capacity, and operational interoperability. These characteristics are reinforced by the role of ENISA in developing certification schemes, facilitating regulatory coordination, and supporting the implementation of cybersecurity obligations across the digital single market. The gradual expansion of ENISA's operational responsibilities under recent EU cybersecurity legislation further reflects the increasing institutionalization of preventative based cybersecurity governance within the Union.[355]

At the same time, the EU model also exposes important proportionality and implementation challenges. The introduction of mandatory certification and conformity assessment obligations generates substantial compliance burdens for economic operators, particularly SMEs. Compliance costs extend beyond initial product development and include technical documentation, conformity assessments, continuous monitoring, vulnerability handling, and ongoing reporting obligations.[356] This challenge is further compounded by global market asymmetries, as manufacturers operating in jurisdictions with less stringent cybersecurity requirements must bear full compliance costs under a mandatory European certification regime.

Official EU data underscores the anticipated financial impact of implementing this regulatory regime. According to the European Commission's impact assessment of the CRA, the preferred regulatory option is expected to generate additional compliance and enforcement costs for businesses, notified bodies, and public authorities, including activities such as notification, accreditation, and market-surveillance.[357]

For software developers and hardware manufacturers, these costs encompass direct compliance expenditures related to new cybersecurity requirements, conformity assessment, technical documentation, and reporting obligations. The assessment estimates that aggregated compliance costs could reach approximately €29 billion for products with digital elements,

[355] European Union Agency for Cybersecurity, The Cyber Resilience Act (CRA) introduces the Single Reporting Platform (SRP) for cybersecurity incident reporting in the EU Digital Single Market, available at https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp, (Accessed 7 April 2026).
[356] BURRI – ZIHLMANN, 2023, B20.
[357] European Commission, Cyber Resilience Act – Impact Assessment, report/study, 15 September 2022, available at https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment, (Accessed 9 April 2026).

representing a market value of up to €1,485 billion in turnover. As a result, end users including businesses, consumers, and public sector entities may face higher prices for digital products.[358]

Empirical research indicates that this financial impact is distributed unevenly across industrial actors. It demonstrates that 50% of surveyed participants expect additional compliance costs to remain below 20% of their current product development budgets, indicating that many firms anticipate being able to absorb new requirements without dramatic increases in expenditure. Meanwhile, 25% of participants estimated that compliance costs could rise by 20–40%, reflecting a moderate financial impact for some entities, and another 25% anticipated no significant change to their costs, suggesting either existing preparedness or the expectation of integrating compliance efforts within existing resource structures.[359] These findings illustrate a broader challenge within mature cybersecurity regulatory systems: balancing legal sophistication and enforceability against economic sustainability and practical market feasibility.

In contrast, the Jordanian cybersecurity framework does not currently establish a dedicated certification regime for digital products comparable to the EU model. This reflects a comparatively lower level of regulatory maturity in relation to legal bindingness and institutional specialization. Nevertheless, the absence of a highly complex certification framework should not necessarily be viewed solely as a regulatory deficiency. Rather, it also reflects the practical realities of institutional capacity constraints, resource limitations, and the developmental stage of Jordan's cybersecurity ecosystem.

The implementation of advanced certification mechanisms in Jordan would require substantial technical infrastructure, specialized expertise, accreditation systems, and sustained financial investment. Current institutional and budgetary limitations indicate that the establishment of comprehensive conformity assessment structures comparable to those within the EU would present significant practical challenges. Accordingly, the regulatory gap should be assessed not only in terms of the absence of binding certification obligations, but also in light of the institutional capacity required to implement and supervise such a regime effectively.

---

[358] Ibid.

[359] Risto, Roosa – Sethi, Mohit – Katara, Mika, Effects of the Cyber Resilience Act (CRA) on Industrial Equipment Manufacturing Companies, 11 October 2025, available at https://arxiv.org/html/2505.14325v2, (Accessed 9 April 2026).

Furthermore, the introduction of highly demanding certification obligations could disproportionately affect Jordanian SMEs, many of which operate with limited cybersecurity resources and technical capacity. This concern is supported by empirical research conducted in Saudi Arabia-an Arab country facing comparable economic and structural challenges-which has shown that small enterprises continue to struggle with the implementation of adequate cybersecurity measures, primarily due to the high cost of cybersecurity solutions.[360]

In this context, similar regulatory dynamics in Jordan could disproportionately affect SMEs, potentially increasing barriers to market entry, reducing competitiveness, and slowing the pace of innovation within the domestic digital sector. This consideration also engages the proportionality and private-sector engagement dimensions of the Regulatory Maturity Matrix, since a certification regime must balance the achievement of security objectives against the regulatory and financial burdens imposed on market actors.

Measured against the Regulatory Maturity Matrix, the EU framework distributes binding preventative responsibilities across relevant market actors and supports them through specialized institutions and interoperable mechanisms. By contrast, Jordan's framework remains less formalized at the product level, with greater reliance on centralized administrative oversight and organizational compliance.

Accordingly, the EU framework is classified as High maturity, while Jordan falls within the Nascent/Low maturity tier in digital-product certification. This classification reflects Jordan's absence of a dedicated, legally binding, and institutionally developed product-certification regime comparable to the EU model, rather than the maturity of its cybersecurity framework as a whole.

V.3.2 Risk Management Frameworks

Risk management constitutes a foundational component of contemporary cybersecurity governance, reflecting the transition from reactive security models toward anticipatory, resilience-oriented regulatory approaches. Within the EU, this paradigm is most comprehensively articulated under the NIS2 Directive, which establishes a structured and risk-based framework imposing legally binding cybersecurity obligations on both essential and important entities.[361] By contrast,

[360] ALHARBI et al., 2021, p.12.
[361] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 21(1).

the Jordanian approach, primarily grounded in the Jordanian Cybersecurity Law No. 16 of 2019, remains comparatively general and policy-driven, relying on centralized institutional oversight rather than detailed and enforceable risk management obligations.

Under Article 21 of the NIS2 Directive, entities are required to implement "appropriate and proportionate technical, operational, and organizational measures" to manage risks to network and information systems.[362] This formulation places the principle of risk proportionality at the center of the EU cybersecurity model, ensuring that compliance obligations are calibrated according to organizational scale, sector criticality, and threat severity.

The Directive further adopts an integrated "all-hazards" approach encompassing multiple interrelated domains, including incident handling, supply chain security, vulnerability management, encryption, access control, and business continuity planning.[363] In doing so, the EU framework conceptualizes cybersecurity risk as systemic and interconnected rather than confined to isolated technical threats.

The incorporation of continuous risk assessment obligations under the NIS2 directive reflects an advanced regulatory approach in which cybersecurity governance is embedded within broader organizational and operational processes rather than treated as an *ex-post* function. Moreover, the emphasis on proportionality enhances regulatory adaptability by allowing entities to tailor compliance measures according to evolving technological and sector-specific threat profiles.[364]

Nevertheless, the EU framework also reveals important structural and operational complexities. The breadth of obligations imposed under the NIS2 Directive, combined with the absence of fully harmonized technical standards, generates interpretative uncertainty for regulated entities. While the Directive encourages alignment with European and international standards, it does not prescribe a uniform set of binding technical requirements applicable across all sectors. This creates a degree of implementation variability that may affect regulatory consistency between Member States and across industries.

[362] Ibid., Article 21(2).
[363] Ibid.
[364] VANDEZANDE, 2024, p.11.

These complexities are further reinforced by the interaction between the NIS2 Directive and the CRA. While the NIS2 Directive encourages Member States to align with international standards[365] and promotes the exchange of best practices,[366] its primary regulatory focus is on establishing organizational risk-management obligations for essential and important entities rather than setting detailed technical standards for hardware and software.

In contrast, the CRA establishes highly prescriptive conformity and product-security requirements for hardware and software with digital elements. However, the practical operationalization of these CRA mandates remains fundamentally dependent on the formal adoption of harmonized technical standards and standardized conformity assessment procedures.[367] Consequently, the coexistence of overlapping regulatory instruments may create uncertainty concerning the interpretation and operationalization of cybersecurity obligations, particularly where entities must simultaneously navigate organizational risk-management duties under NIS2 and product-security requirements under CRA.[368]

On the other hand, the Jordanian cybersecurity framework adopts a more centralized and policy-driven model. Article 6/B/1 of the Cybersecurity Law assigns the NCSC responsibility for developing national strategies, standards, and policies, as well as supervising their implementation.[369] Although this provides a foundational governance structure, the primary statute does not establish a comprehensive, legally binding risk management regime comparable to the NIS2 Directive. Specifically, primary Jordanian legislation does not articulate explicit statutory risk categories, mandate periodic risk audits, or impose structured duties regarding continuous supply chain risk management.

These operational limitations are illustrated by empirical findings from a case study conducted at the University of Jordan evaluating a compliance and capability assessment tool aligned with the Jordanian National Cybersecurity Framework. The study identified several

[365] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 25.
[366] Ibid., Article 14 (4)(C).
[367] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), Article 19.
[368] Ruohonen, Jukka, A Systematic Literature Review on the NIS2 Directive, 2024, available at https://arxiv.org/pdf/2412.08084, (Accessed 14 April 2026).
[369] Jordan, Cybersecurity Law No. 16 of 2019, Article 6(B)(1).

operational shortcomings, including the absence of clearly interpretable controls, limited risk-prioritization mechanisms, and a heavy reliance on organizational self-assessment.[370]

Because the framework depends heavily on subjective, user-driven interpretation rather than predefined statutory benchmarks, regulated entities are forced to rely on extensive customization and supplementary administrative guidance. This structural reliance on internal interpretation effectively shifts the burden of risk calibration onto individual organizations, resulting in significant implementation variance across sectors and ultimately compromising the coherence of national cybersecurity resilience.

From a broader regulatory perspective, cybersecurity risk management presents distinctive legal challenges due to the technical complexity of digital threats and reliance on dynamic operational data. Unlike traditional operational risks, cyber risks require continuous adaptation, technical expertise, and real-time monitoring. This complexity is particularly visible in highly regulated sectors such as banking and critical infrastructure, where cybersecurity obligations intersect with broader operational risk frameworks.

For instance, in the Jordanian financial sector, commercial banks are required by the Central Bank of Jordan to manage credit, market, and operational risks while simultaneously adhering to specialized cybersecurity frameworks.[371] However, cybersecurity risks present unique regulatory challenges due to their technical volatility and reliance on complex threat intelligence. In practice, fragmented data environments, limited technical interoperability, and the absence of standardized statutory metrics complicate administrative oversight and corporate compliance.

In this context, effective cybersecurity governance depends upon the ability of regulators to translate highly technical risk indicators into measurable legal obligations and enforceable compliance standards. In practice, cybersecurity risk management relies heavily on technical data derived from IT systems, network logs, and dynamic threat indicators, which are not easily accessible or interpretable within traditional legal and regulatory frameworks.

This gap creates substantial complexity for administrative authorities tasked with defining clear statutory obligations, verifying compliance, and establishing objective assessment metrics.

[370] ALMOMANI et al., 2026, p. 29.
[371] Central Bank of Jordan, Cybersecurity Framework for Jordan Financial Sector, Version 1.0, July 2021, available at https://www.cbj.gov.jo/EBV4.0/Root_Storage/EN/CSF4JFSv1-0.pdf, (Accessed 18 April 2026).

The widespread fragmentation of data sources, coupled with a lack of technical interoperability between operational IT systems and legal compliance frameworks, further complicates administrative oversight and corporate compliance.

Measured against the evaluative criteria of the Regulatory Maturity Matrix, the two systems diverge fundamentally in legal bindingness, operational specificity, and risk proportionality. The EU framework reflects a highly institutionalized and operationally integrated model of cybersecurity risk governance characterized by legal enforceability, risk proportionality, resilience integration, and continuous adaptation mechanisms, classifying it as high maturity. However, the operational complexity and resource intensity of this supranational model illustrate the significant institutional capacity required to sustain such a regime.

By contrast, the Jordanian framework establishes a formal institutional baseline through the Cybersecurity Law, the active operational presence of the NCSC, national strategies, and developing sectoral risk practices. However, because it remains constrained by broad executive discretion, centralized administrative governance, limited statutory specificity, and a heavy reliance on organizational self-assessment rather than mandatory, risk-calibrated benchmarks, Jordan's risk management framework falls within the medium maturity tier.

Consequently, the comparative evidence highlights a fundamental structural gap: while Jordan possesses the foundational institutional architecture necessary for national oversight, its legal model relies on abstract policy guidelines rather than the enforceable, risk-calibrated statutory standards required to achieve the high regulatory maturity and comprehensive resilience demonstrated by the EU regime.

V.3.3 Security of Data Processing as a Preventative Measure

The security of data processing constitutes a central preventative mechanism within contemporary cybersecurity governance, reflecting the recognition that the protection of data confidentiality, integrity, and availability must be embedded within the operational architecture of digital systems. Within the EU, this principle is most prominently articulated under Article 32 of the GDPR, which requires controllers and processors to implement appropriate technical and organizational measures ensuring a level of security commensurate with the risks associated with data

processing.[372] By contrast, the Jordanian framework, as established under Article 8(b) of the Jordanian PDPL, adopts a prescriptive approach, imposing security obligations without clearly embedding a proportional, risk-based methodology.[373]

The EU framework is fundamentally grounded in the principle of risk proportionality. Under the GDPR, organizations are required to assess the likelihood and severity of risks to the rights and freedoms of individuals and to calibrate security measures accordingly. This includes, where appropriate, the implementation of encryption, pseudonymization, access controls, and the regular testing and evaluation of system effectiveness. This approach reflects a broader regulatory understanding that cybersecurity obligations cannot be uniformly applied across all processing activities, but must instead remain responsive to the nature of the data processed, the scale of operations, and the evolving threat landscape.[374]

From the perspective of the Regulatory Maturity Matrix, the EU model demonstrates a high degree of risk proportionality, operational adaptability, and resilience integration. By embedding continuous risk assessment within legally binding obligations, the GDPR establishes a flexible governance framework in which security measures can be adapted to diverse technological environments and evolving threat landscapes. In this respect, processing security functions not merely as a static compliance requirement, but as a dynamic risk management process integrated throughout organizational operations.[375]

Nevertheless, the flexibility inherent in the EU model also introduces certain operational and interpretative challenges. The absence of exhaustive or universally binding technical standards may result in divergent implementations across sectors and organizations, particularly where entities lack sufficient technical expertise or institutional capacity to conduct sophisticated risk assessments.[376] Consequently, while the GDPR enhances adaptability and technological neutrality, its effective operation depends heavily on organizational competence, regulatory guidance, and consistent administrative enforcement.

---

[372] European Parliament and Council of the European Union, Regulation No. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), Article 32.
[373] Jordan, PDPL No. 24 of 2023, Article 8(b).
[374] HOLZENBERGER – MAXWELL, 2025, p.4.
[375] WAQDAN et al., 2025, p.12.
[376] SMIRNOVA – TRAVIESO-MORALES, 2024, p.337.

In contrast, the Jordanian legal framework adopts a more rigid, compliance-oriented model. Article 8 of the PDPL requires controllers and processors to implement strict data security measures without explicitly incorporating the principle of proportionality or providing guidance on risk-based calibration.[377] While this prescriptive structure establishes clear baseline expectations, it lacks statutory differentiation.[378]

Consequently, the imposition of uniform obligations lacking risk-based weighting generates two distinct governance vulnerabilities: first, low-risk entities are subjected to disproportionately burdensome technical requirements, resulting in operational over-compliance,[379] and second, entities managing highly sensitive assets are deprived of tailored safeguards for high-risk operations, resulting in systemic under-protection. This formalistic regulatory approach constrains operational flexibility, contrasting sharply with the continuous risk-evaluation paradigm characteristic of the European model.

Measured against the evaluative criteria of the Regulatory Maturity Matrix, the comparison indicates that the EU framework provides a highly differentiated, legally integrated, and risk-calibrated model of preventative data security governance, classifying it as high maturity. In contrast, the Jordanian framework establishes formal, binding statutory security mandates under Article 8 of the PDPL, but remains comparatively constrained in risk calibration, operational flexibility, and contextual responsiveness, placing it within the medium maturity tier. The divergence is therefore not a matter of the complete absence of security obligations, but of the extent to which those statutory duties are legally differentiated, adaptable, and integrated into continuous, risk-based governance.

V.4 Reactive Cybersecurity Mechanisms (During incident)

Reactive cybersecurity mechanisms constitute a fundamental component of contemporary cybersecurity governance, complementing preventative strategies by addressing incidents once they occur. Whereas preventative measures seek to reduce vulnerabilities and minimize the likelihood of cyber intrusions, reactive mechanisms focus on detecting, reporting, containing, and mitigating cybersecurity incidents after systems have been compromised. These mechanisms are

[377] Jordan, PDPL No. 24 of 2023, Article 8.
[378] KUZMINYKH et al., 2022, p.55.
[379] BLACK – BALDWIN, 2012, p.15.

particularly significant within increasingly interconnected digital environments, where delayed detection or fragmented response structures may substantially amplify operational, economic, and societal harm.

From a governance perspective, reactive cybersecurity regulation extends beyond technical incident handling to encompass broader institutional coordination, information sharing, and regulatory accountability. Mechanisms such as cyber incident reporting and breach notification therefore play a critical role in enhancing situational awareness, facilitating coordinated responses, and strengthening systemic resilience across both public and private sectors. As reflected in the Regulatory Maturity Matrix, the effectiveness of reactive governance mechanisms depends largely on procedural clarity, operational interoperability, legal bindingness, and institutional coordination capacity.

V.4.1 Cyber Incident Reporting Systems

Cyber incident reporting systems constitute a central pillar of reactive cybersecurity governance, enabling the timely detection, assessment, and coordinated management of cybersecurity incidents. As cyber threats become increasingly sophisticated and transnational in nature, reporting mechanisms perform essential regulatory functions by enhancing threat visibility, facilitating information exchange, and supporting both national and cross-border response coordination.[380] From a legal and governance perspective, effective reporting frameworks must balance the need for rapid disclosure with operational feasibility, ensuring that reporting obligations remain both proportionate and sufficiently precise to support consistent implementation.

Within the EU, the original NIS Directive established a mandatory requirement for covered entities to report security breaches. Incident reporting, also referred to as security breach notification, is considered a cornerstone of the EU cybersecurity legislation.[381] However, under the Directive, the criteria for reporting significant cybersecurity incidents were relatively vague, focusing on factors such as the number of users affected, the duration of the disruption, and its geographical spread. This lack of precision often resulted in inconsistent interpretation across

[380] ZAMFIROIU – SHARMA, 2022, p.71.
[381] SCHMITZ-BERNDT, 2023, p.2.

Member States and led to underreporting by entities uncertain about what constituted a "significant" incident.[382]

The NIS2 Directive addresses these shortcomings by introducing a more structured, multi-stage reporting process and refining the criteria for significance. Incidents are defined as events compromising the confidentiality, integrity, availability, or authenticity of data or related services. Under Article 23, essential and important entities are required to submit an early warning within 24 hours of becoming aware of a significant incident, followed by a formal incident notification within 72 hours and a final report within one month. This phased reporting structure reflects a more mature and operationally integrated approach to cybersecurity governance, enabling prompt regulatory awareness while preserving sufficient flexibility for organizations to refine assessments as technical investigations develop.[383]

From the perspective of the Regulatory Maturity Matrix, the NIS2 regime demonstrates a high degree of legal bindingness, operational interoperability, and resilience integration. The introduction of structured reporting timelines, graduated notification stages, and harmonized procedural requirements strengthens both institutional coordination and cross-border situational awareness. At the same time, the EU framework reflects a coordinated approach to reactive cybersecurity governance, in which incident reporting obligations directly feed into broader resilience and institutional response mechanisms managed by national CSIRTs and the EU-CyCLONe network.

In parallel, the CRA introduces a distinct reporting regime applicable to products with digital elements. Under Article 14 of the CRA, manufacturers are required to follow a staged reporting model, submitting an early warning within 24 hours of becoming aware of an actively exploited vulnerability or severe incident, a subsequent notification within 72 hours, and a final report once remediation or mitigation is deployed.[384]

Furthermore, CRA reporting obligations operate independently from NIS2 incident reporting and data breach notification requirements under the GDPR. This regulatory separation

[382] VANDEZANDE, 2024, p.8.
[383] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 23(1).
[384] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), Article 14(1).

establishes a multi-layered compliance environment in which a single security incident may trigger parallel, multi-stage reporting duties across distinct legal instruments.

While this layered structure enhances regulatory coverage and strengthens systemic visibility over cybersecurity risks, it also introduces significant operational complexity. The coexistence of multiple reporting regimes may generate interpretative uncertainty, duplicative compliance burdens, and coordination challenges for entities operating across different sectors and regulatory frameworks. Consequently, the effectiveness of the EU model depends heavily upon advanced institutional coordination, standardized reporting taxonomies, and administrative capacity capable of managing overlapping regulatory obligations coherently.

By contrast, the Jordanian cyber incident reporting framework remains characterized by a structural reliance on administrative instruments rather than a lack of regulatory initiative altogether. The formal legal obligation to notify the NCSC is established under primary legislation,[385] and reinforced by the Instructions for Determining the Criteria for Violations of the Provisions of the Cybersecurity Law, which provides administrative penalties for failing to report incidents affecting national cyberspace.[386] However, at the level of primary statutory enactment, the legislative framework does not codify explicit thresholds of significance, graduated procedural stages, or legally binding notification deadlines comparable to the statutory architecture of the NIS2 Directive.

To regulate these operational dimensions, Jordan has also established a national cybersecurity incident reporting platform intended to facilitate submissions by public entities, private organizations, and individuals.[387] The NCSC issued the Cyber Security Incident Response and Reporting Policy 2025, which articulates severity-based classifications and establishes baseline operational response timelines. However, because this instrument remains an administrative policy rather than a comprehensive primary legislative enactment, it lacks the

[385] Jordan, Cybersecurity Law No. 16 of 2019, Article 8(b)(3).
[386] Jordan, Instructions for Determining the Criteria for Violations of the Provisions of the Cybersecurity Law, Their Controls and the Procedures Due Thereto for the Year 2025, Article 6(A)(12).
[387] YOUNES et al., 2024, p.824.

broader normative force, procedural depth, and binding statutory enforceability required to ensure consistent compliance across all sectors.[388]

Recent regulatory developments, including the issuance of licensing instructions governing cybersecurity-related services such as managed security services, incident response, consulting, auditing, and training, reflect an emerging effort to structure the cybersecurity sector institutionally.[389] Nevertheless, these measures primarily regulate professional accreditation and service provision rather than establishing comprehensive substantive obligations concerning cyber incident disclosure and coordinated reporting governance.

Measured against the Regulatory Maturity Matrix, the divergence centers upon legal bindingness, procedural clarity, and operational interoperability. The EU framework demonstrates an integrated structured timelines and phased reporting within a legally enforceable supranational system, thereby classifying it as high maturity. By contrast, the Jordanian framework establishes a formal institutional baseline via statutory notification duties. However, constrained by secondary administrative reliance and limited primary statutory specificity, Jordan falls within the medium maturity tier for cyber incident reporting.[390]

This structural reliance on administrative policies rather than primary statutory codification creates a lower baseline of normative certainty and procedural enforceability relative to the EU's harmonized legislative architecture, highlighting the gap between executive guidelines and enforceable statutory frameworks in reactive cybersecurity governance.[391]

V.4.2 Personal Data Breach Notification

Personal data breach notification constitutes a critical component of reactive cybersecurity governance, operating at the intersection of data protection and cybersecurity regulation. While

---

[388] Jordan, the National Cybersecurity center, Cybersecurity Incident Response and Reporting Policy 2025, available at https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/cs_incident_response_and_reporting_policy_2025-0.pdf, (Accessed 1 May 2026).

[389] Jordan, Instructions for Licensing Cybersecurity Competitions Services for the Year 2026, Instructions for Licensing Managed Cybersecurity Services for the Year 2026, Instructions for Licensing Cybersecurity Consulting Services for the Year 2026, Instructions for Licensing Cybersecurity Training Services for the Year 2026, Instructions for Licensing Cybersecurity Incident Response Services for the Year 2026, Instructions for Licensing Cybersecurity Products Sales Services for the Year 2026, and Instructions for Cybersecurity Audit Services for the Year 2026. Available at https://www.pm.gov.jo/Ar/Pages/NewsPaperDetails/6039 (Accessed 19 April 2026).

[390] SEN, 2023, p.328.

[391] BUSETTI – SCANNI, 2024, p.4.

cyber incident reporting mechanisms under NIS2 primarily aim to enhance systemic threat visibility and coordinated operational response, breach notification regimes focus specifically on protecting the rights and freedoms of individuals affected by security incidents involving personal data. As such, they represent a complementary, distinct layer of regulatory response within broader cybersecurity governance frameworks.

Within the EU, breach notification is governed by Articles 33 and 34 of the GDPR, which establish a tiered, risk-based and proportionate reporting regime.[392] Under this framework, data controllers are required to notify the competent supervisory authority within 72 hours of becoming aware of a personal data breach, but only where the breach is likely to result in a risk to the rights and freedoms of natural persons. Direct notification to affected data subjects is mandated exclusively in instances where the incident is likely to result in a high risk, thereby introducing a calibrated threshold that distinguishes between varying degrees of severity and potential harm.

From the perspective of the Regulatory Maturity Matrix, the GDPR framework demonstrates a high degree of risk proportionality, operational adaptability, and legal enforceability.[393] By linking statutory notification obligations directly to the likelihood and severity of harm, the EU model integrates legal compliance with contextual risk assessment, thereby enabling a more calibrated and operationally sustainable reporting system by reducing the likelihood of "notification fatigue" among both regulators and data subjects. This approach also minimizes unnecessary regulatory burdens by limiting mandatory notifications to incidents with material impact on affected individuals.

The EU framework is further reinforced by detailed interpretative guidance issued by the European Data Protection Board (EDPB), enhancing legal certainty and cross-border consistency across Member States.[394] Nevertheless, the flexibility inherent within the GDPR model presents distinct operational challenges. The effectiveness of a risk-based notification regime depends heavily upon the technical and organizational capacity of data controllers to conduct timely,

[392] European Parliament and Council of the European Union, Regulation No. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), (Articles 33, 34).
[393] DE-YOLANDE et al., 2023, p.344.
[394] European Data Protection Board, Guidelines 01/2021 on Examples regarding Data Breach Notification, Version 2.0, 14 December 2021, published in 2022, available at https://www.edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf, (Accessed 22 April 2026).

accurate forensic risk assessments, which may vary considerably according to institutional capacity, technical expertise, and sectoral resources. Consequently, practical implementation may produce interpretative divergence and inconsistent reporting practices across organizations and sectors, particularly where entities lack specialized data protection expertise.

In contrast, the Jordanian legal framework conditions its breach-notification obligations on a specific harm threshold. Under Article 20(A) of the Jordanian PDPL, the mandatory duties to notify affected individuals within 24 hours and report to the Data Protection Unit within 72 hours are triggered only when a security breach is likely to lead to severe harm to the data subject.[395] While this establishes a risk-oriented trigger rather than a strict 'all-incident' rule, the statutory threshold relies heavily on a high-water mark of 'severe harm' (similar to the GDPR's high risk to rights and freedoms standard under Article 34, yet textually focused on severe tangible or intangible impact), leaving interpretive weight to administrative guidance to define how controllers should calibrate lesser anomalies.[396]

From a regulatory design perspective, the reliance on a binary "severe harm" threshold within the Jordanian framework creates distinct operational complications: First, because Article 20(A) sets a high-water mark of potential severe harm without providing granular, sector-specific risk-assessment criteria, controllers face significant ambiguity regarding whether borderline incidents meet the mandatory reporting threshold.[397]

Furthermore, while the strict 24-hour and 72-hour windows prioritize accelerated disclosure, the lack of a tiered risk-filtering mechanism—such as the EU's calibration between "risk" and "high risk" to rights and freedoms—leaves little room to scale responses according to varying degrees of severity. However, the direct transplantation of flexible European risk thresholds into Jordan requires caution; effective risk-based regimes demand extensive regulatory guidance, institutional expertise, and supervisory consistency to prevent subjective underreporting.

Measured against the evaluative criteria of the Regulatory Maturity Matrix, the two legal orders diverge significantly across risk proportionality, legal bindingness, and enforcement

[395] Jordan, PDPL No. 24 of 2023, Article 20(A).
[396] European Parliament and Council of the European Union, Regulation No. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), Article 34.
[397] KUZMINYKH et al., 2022, p.55.

mechanisms. The EU model integrates contextual risk assessment with legally enforceable, tiered disclosure mandates supported by administrative guidelines, classifying it as high maturity. In contrast, while the Jordanian regime establishes a binding statutory framework under the PDPL, it relies on a rigid severe-harm trigger without intermediate contextual differentiation. Because it remains limited in operational flexibility, Jordan falls within the medium maturity tier for personal data breach notification, thereby demonstrating that its regulatory constraint stems from statutory rigidity rather than a total absence of obligations.

V.5 Post-Incident Cybersecurity Mechanisms

Post-incident mechanisms constitute a critical dimension of cybersecurity governance, focusing on system recovery, remediation, and the integration of institutional learning into ongoing security operations. Whereas reactive mechanisms address the immediate containment and mitigation of active security incidents, post-incident governance is concerned with restoring system integrity, mitigating residual vulnerabilities, ensuring business continuity, and preventing incident recurrence. In this respect, contemporary cybersecurity governance extends beyond immediate operational response to encompass broader structures of regulatory accountability and institutional learning.

Remediation refers to the structured process through which operational control over a compromised information system is re-established and the system is restored to a secure operational baseline following a cybersecurity incident.[398] This process encompasses service restoration, malware eradication, vulnerability patching, and the execution of corrective measures designed to mitigate future systemic risk. Remediation thus functions as an operational bridge connecting active incident response to long-term resilience governance.

Within the EU, post-incident remediation is embedded within a legally binding regulatory framework, principally under the NIS2 Directive. Although the Directive does not define remediation as an isolated statutory concept, it imposes enforceable obligations requiring regulated entities to restore the security, integrity, and continuity of network and information systems following an incident. Under Article 23 of the NIS2 Directive, essential and important entities must

[398] Agence nationale de la sécurité des systèmes d'information (ANSSI): Cyber Attacks and Remediation: Managing the Remediation, available at https://messervices.cyber.gouv.fr/documents-guides/cyber-attacks-remediation-managing-remediation.pdf (Accessed 29 April 2026).

submit a comprehensive final incident report within one month of notification, detailing recovery measures undertaken and long-term corrective configurations implemented.[399] These obligations are reinforced by substantial administrative penalties under Article 34, transforming post-incident recovery into a legally enforceable governance duty.[400]

Furthermore, under Article 21(1) and Article 21(2)(b)–(c) of the NIS2 Directive, regulated entities are required to integrate comprehensive risk-management measures—including incident handling, business continuity, backup management, and disaster recovery planning—into their core security operations.[401] Rather than treating recovery as an isolated post-incident technical activity, the European framework embeds these safeguards within a broader statutory risk-management obligation, with specific operational standards and audit mechanisms further calibrated by national supervisory authorities and an entity's individual risk profile.[402]

By contrast, the Jordanian cybersecurity framework lacks a comprehensive, legally binding regime governing post-incident remediation and recovery. The primary legal framework relies on administrative instruments, most notably the Cybersecurity Incident Response and Reporting Policy 2025 issued by the NCSC.[403] While this policy establishes procedural guidelines for detection, containment, eradication, and system restoration, it operates as an administrative policy rather than a binding primary statute. Consequently, post-incident measures remain operational recommendations rather than legally enforceable statutory duties.

Although the 2025 Policy references post-incident evaluation and lessons-learned exercises, these procedures are not linked to statutory compliance audits, mandatory root-cause disclosures, or formal remediation verification structures comparable to the NIS2 framework.[404] While operational response timelines are established based on incident severity, the Jordanian framework does not impose equivalent statutory obligations concerning mandatory disaster

[399] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 23(4)(d).
[400] Ibid., Article 34.
[401] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article (21(1), (2) (b-C)).
[402] TAHMASEBI, 2024, p.119.
[403] Jordan, the National Cybersecurity Center, Cybersecurity Incident Response and Reporting Policy 2025, available at https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/cs_incident_response_and_reporting_policy_2025-0.pdf, (Accessed 2 May 2026).
[404] Ibid., Article 8.

recovery testing, business continuity audits, or systematic resilience verification.[405] The absence of such mechanisms also limits institutional oversight capacity and reduces the ability of competent authorities to evaluate the effectiveness of organizational remediation efforts consistently.[406]

These structural limitations are corroborated by empirical research within the Jordanian context, which highlights the absence of standardized, objective mechanisms for assessing organizational compliance with national cybersecurity and recovery frameworks.[407] Existing compliance oversight remains reliant on subjective organizational self-assessment and voluntary administrative reporting, which constrains supervisory verification capacity and increases the risk of implementation variance across sectors.

Measured against the evaluative criteria of the Regulatory Maturity Matrix, the structural divergence between the two frameworks centers upon legal bindingness, resilience integration, and institutional accountability. The EU model embeds post-incident recovery within a legally binding statutory regime supported by mandatory final reporting, and administrative sanctioning powers, classifying it as High maturity.

Conversely, the Jordanian framework exhibits a relative absence of a comprehensive statutory architecture for post-incident governance. Relying primarily on centralized administrative guidance, voluntary operational compliance, and unverified self-assessment without statutory root-cause disclosures or disaster recovery audits, Jordan falls within the Low maturity tier for post-incident mechanisms. This structural deficit reflects a transitional regulatory baseline lacking the enforceable statutory structures required to sustain a continuous, closed-loop resilience cycle.

V.6 Cross-Cutting Cybersecurity Mechanisms: Toward Lifecycle-Based Governance

Beyond traditional stage-based regulation, contemporary EU cybersecurity frameworks demonstrate a clear transition toward cross-cutting governance mechanisms that operate continuously across the digital ecosystem. Rather than functioning solely within discrete preventative, reactive, or post-incident phases, these mechanisms embed cybersecurity as an

[405] Ibid., Article 7.
[406] ALMOMANI et al., 2026, p.29.
[407] Ibid.

ongoing, lifecycle-oriented regulatory condition within digital networks. This evolution reflects a broader paradigm shift from fragmented, incident-driven intervention toward continuous resilience architectures.

Measured against the evaluative criteria of the Regulatory Maturity Matrix, this transition is defined by the growing centrality of lifecycle continuity, operational interoperability, and private-sector engagement. Advanced regulatory models conceptualize cybersecurity not as a periodic compliance checkpoint, but as a permanent governance process requiring sustained coordination among statutory authorities, economic operators, and technical infrastructures.

This cross-cutting governance architecture encompasses three interrelated dimensions: continuous vulnerability governance and secure development (Section V.6.1), lifecycle-based digital product security regulation (Section V.6.2), and systemic resilience and cyber solidarity mechanisms (Section V.6.3). Collectively, these mechanisms illustrate the consolidation of an integrated regulatory model that governs digital systems across their entire operational lifespan.

V.6.1 Continuous Vulnerability Governance and Secure Development

A central feature of lifecycle-based cybersecurity governance is the institutionalization of mechanisms that treat vulnerabilities as an ongoing regulatory concern rather than as isolated technical defects addressed only after cybersecurity incidents occur. In this context, coordinated vulnerability disclosure (CVD) frameworks reflect an emerging governance approach aimed at strengthening the cyber resilience of ICT products and services through continuous processes of vulnerability identification, reporting, coordination, mitigation, and disclosure. This approach is premised on the understanding that vulnerabilities must be systematically integrated within broader governance and information-sharing structures rather than relying exclusively on post-incident remediation.[408]

Within the EU, this transition is prominently established under the NIS2 Directive, which formalizes a structured framework for vulnerability coordination and disclosure. [409] In particular, a competent CSIRT in each Member State acts as a coordinator and trusted intermediary. This designated CSIRT is responsible for facilitating communication between vulnerability reporters

[408] GIANNAKOULIAS, 2023, p.41.
[409] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 12.

and manufacturers or providers of ICT products or services, assisting reporters, negotiating disclosure timelines, and managing vulnerabilities that affect entities across multiple Member States.[410]

The NIS2 framework further supports this approach by introducing procedural safeguards for coordinated vulnerability reporting. In particular, Article 12(1) requires Member States to ensure that natural or legal persons may report vulnerabilities anonymously where they so request, while explicitly obliging the designated coordinating CSIRT to protect the anonymity of the reporter.[411]

At the supranational level, the role assigned to ENISA under Article 12(2) in developing and maintaining a European vulnerability database further reinforces this information-sharing infrastructure.[412] By establishing a Union-level repository concerning publicly known vulnerabilities in ICT products and services, the database functions as a shared informational mechanism supporting coordinated awareness and the dissemination of security mitigation measures across the Union.

Taken together, these mechanisms demonstrate how vulnerability management is no longer confined to post-incident remediation but is instead embedded throughout the entire cybersecurity lifecycle. The combination of coordinated disclosure frameworks and shared informational infrastructures contributes to a model of continuous vigilance, in which vulnerabilities are systematically integrated into regulatory oversight, organizational practices, and technical development processes.

By contrast, the Jordanian approach to coordinated vulnerability governance remains comparatively underdeveloped at both the institutional and regulatory levels. Although Jordan has not yet established a comprehensive legal framework for CVD comparable to that under the NIS2 Directive, elements of resilience-oriented vulnerability governance can nevertheless be identified within the national cybersecurity framework. In particular, the Jordanian National Cybersecurity

[410] Ibid., Article 12(1).
[411] Ruohonen, Jukka: A Systematic Literature Review on the NIS2 Directive, arXiv preprint, 2024, available at https://arxiv.org/html/2412.08084v1 (Accessed 5 May 2026).
[412] Ibid., Article 12(2).

Strategy 2025–2028 reflects an increasing emphasis on cyber resilience, proactive risk management, institutional coordination, and capacity building.[413]

Within this framework, the NCSC and the national Computer Emergency Response Team (JoCERT) perform important operational functions relating to cybersecurity incident response and national preparedness.[414] However, these strategic measures remain policy-oriented and do not establish a formalized CVD regime, or a centralized national vulnerability database comparable to the EU model. Moreover, unlike the European framework under Article 12 of the NIS2 Directive, the Jordanian system does not provide statutory procedural guarantees for security researchers, such as mechanisms for anonymous reporting or formalized disclosure protections.

Measured against the evaluative criteria of the Regulatory Maturity Matrix, the divergence between the two frameworks centers upon lifecycle continuity, private-sector engagement, and operational interoperability. The EU framework reflects a mature model of vulnerability governance characterized by statutory lifecycle continuity, structured private researcher engagement, and institutional interoperability via ENISA and national CSIRTs, classifying it as high maturity. By contrast, the Jordanian framework remains strategy-driven, institutionally centralized, and reliant on high-level administrative guidance. Due to the complete absence of a formalized CVD regime, anonymous reporting guarantees, and a national vulnerability database, Jordan falls within the low maturity tier for continuous vulnerability governance.

V.6.2 Lifecycle-Based Product Security Regulation

A second pillar of lifecycle-based cybersecurity governance is the emergence of product-oriented cybersecurity regulation that integrates security obligations throughout the entire lifecycle of ICT products and services. This approach increasingly embeds cybersecurity requirements directly into the design, development, deployment, maintenance, and end-of-life phases of digital products. This reflects a broader transformation from reactive cybersecurity regulation toward a preventive and security-by-design governance model.

---

[413] Jordan's National Cybersecurity Center, National Cybersecurity Strategy 2025–2028, available at https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/national_cybersecurity_strategy_2025-2028_(2).pdf, (Accessed 7 May 2026).

[414] Jordan Computer Emergency Response Team, Mission and Values, available at https://jocert.ncsc.jo/EN/Pages/Mission_and_Values, (Accessed 7 May 2026).

Within the EU framework, this approach is most visibly reflected in the CRA, which establishes horizontal cybersecurity requirements applicable to products with digital elements falling within its defined scope and exemptions.[415] The CRA conceptualizes cybersecurity not as a one-time compliance milestone, but as a continuous process extending across a product's support period. Accordingly, the regulation allocates distinct compliance duties across the supply chain: manufacturers bear the principal responsibility for embedding essential cybersecurity requirements, conducting risk assessments, and managing vulnerabilities throughout the product's lifecycle, whereas importers and distributors are subject to specific verification, due-diligence, and corrective obligations rather than identical lifecycle-wide burdens.[416]

The lifecycle-oriented structure of the CRA is particularly evident within Annex I, which establishes two interconnected categories of obligations. First, the Regulation imposes cybersecurity requirements relating to product design and development, requiring products to be designed, developed, and produced in accordance with security-by-design principles.[417]

Secondly, it establishes extensive vulnerability handling obligations requiring manufacturers to continuously monitor, identify, remediate, and disclose vulnerabilities throughout the designated security support period of products. These obligations extend far beyond initial conformity assessment, embedding cybersecurity governance within ongoing maintenance processes long after products have been placed on the internal market.[418]

The CRA further reinforces this lifecycle approach by requiring manufacturers to determine and clearly specify a security support period that reflects the expected product lifetime, providing security updates and vulnerability patches without additional cost throughout that duration. Manufacturers must also conduct regular security testing, publicly disclose fixed vulnerabilities, facilitate user reporting of vulnerabilities, and notify competent authorities, including national CSIRTs and ENISA, of actively exploited vulnerabilities and severe incidents.[419] Where third-party components are incorporated into products, manufacturers remain

[415] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act).
[416] Ibid., Article 13(2).
[417] Ibid., Annex I, Part 1.
[418] Ibid., Annex I, Part 2.
[419] Ibid., Article 14.

statutorily responsible for ensuring compliance and coordinating vulnerability management obligations throughout the supply chain.

At the same time, the CRA also illustrates the practical and structural challenges associated with highly integrated lifecycle governance models. The obligation to maintain long-term security support and continuous vulnerability management imposes substantial financial, technical, and organizational burdens, particularly on SMEs. Sustained patch management, security testing, compliance monitoring, and ongoing reporting obligations require continuous operational capacity that may not be economically sustainable across all market sectors.

In particular, the requirement to maintain long-term security support raises concerns regarding the emergence of "orphaned" products where manufacturers exit the market, discontinue product lines, or lack sufficient operational resources to maintain ongoing compliance obligations. This reveals an important structural dependency within the CRA framework upon the continued existence and operational capability of manufacturers throughout the lifecycle of digital products.[420]

In addition, the security-by-design model underpinning the CRA raises broader conceptual and operational difficulties. Although the Regulation assumes that cybersecurity risks can be substantially mitigated through anticipatory design and continuous oversight, cybersecurity and cyber resilience remain inherently dynamic and evolving conditions rather than permanently achievable states.[421]

Digital products are rarely static or fully predictable, as they continuously evolve through software updates, modular architectures, third party integrations, and changing patterns of use, thereby limiting the ability of manufacturers to anticipate future vulnerabilities at the design stage. Consequently, while the CRA significantly enhances regulatory integration and long-term resilience management, it also introduces considerable operational complexity and long-term compliance burdens that challenge implementation feasibility.

By contrast, Jordan has not yet adopted binding lifecycle-based cybersecurity obligations applicable to digital products or manufacturers comparable to those established under the CRA.

[420] ORTEGA VELÁZQUEZ et al., 2025, p.20.
[421] BYGRAVE, 2022, p.174.

Nevertheless, the Jordanian National Cybersecurity Strategy 2025–2028 and the Jordan National Cybersecurity Framework increasingly emphasize secure digital transformation, institutional resilience, and the integration of cybersecurity considerations across organizational processes and critical sectors.[422]

Although the Jordanian framework does not currently impose formal statutory obligations concerning security-by-design, lifecycle vulnerability handling, or mandatory long-term patch support,[423] it reflects an emerging policy transition toward resilience-based cybersecurity governance.

Measured against the evaluative criteria of the Regulatory Maturity Matrix, the two legal frameworks diverge fundamentally across the dimensions of lifecycle continuity, legal bindingness, and private-sector engagement. The EU framework reflects a mature and operationally integrated model of lifecycle-based product security governance characterized by legally binding security-by-design obligations, continuous vulnerability handling throughout the product lifespan, and direct regulatory accountability imposed on commercial manufacturers across the supply chain, classifying it as high maturity.

By contrast, the Jordanian framework remains in an initial phase of regulatory development, concentrating its efforts on centralized administrative oversight and public-sector preparedness rather than legally enforceable horizontal product-security duties. Due to the total absence of codified lifecycle obligations, mandatory post-market support mandates, and formal supply chain accountability, Jordan falls within the Low maturity tier for product-level governance. While Jordan demonstrates an increasing strategic awareness of digital resilience, this structural gap highlights a foundational transition phase rather than active product-security regulation.

---

[422] Jordan's National Cybersecurity Center, National Cybersecurity Strategy 2025–2028, available at https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/national_cybersecurity_strategy_2025-2028_(2).pdf, (Accessed 7 May 2026).

[423] National Cybersecurity Center, Jordan National Cybersecurity Framework Capabilities, available at https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/jordan_national_cybersecurity_framework_capabilities.pdf, (Accessed 7 May 2026).

V.6.3 Cyber Solidarity and Systemic Resilience Governance

A third dimension of lifecycle-based cybersecurity governance concerns the emergence of systemic resilience and cyber solidarity mechanisms operating across the full cyber incident lifecycle. This approach emphasizes collective preparedness, coordinated operational response, and institutional cooperation at a broader systemic level. Cybersecurity governance thus evolves beyond the management of individual incidents toward the construction of integrated resilience architectures capable of addressing large-scale cyber threats.

Within the EU approach, this evolution is most prominently reflected in the Cyber Solidarity Act, which demonstrates a transition from purely preventive or reactive cybersecurity regulation toward an integrated resilience-oriented governance model.[424] Rather than regulating cybersecurity incidents as isolated technical events, the Act conceptualizes cyber resilience as a continuous and shared responsibility requiring coordination among supranational institutions, national authorities and trusted MSSPs before, during and after large scale cyber incidents.

Evaluated through the core dimensions of the Regulatory Maturity Matrix, the Cyber Solidarity Act demonstrates an advanced level of operational interoperability, resilience integration, and institutional capacity. Through mechanisms such as the European Cybersecurity Alert System, the Cybersecurity Emergency Mechanism, and the European Cybersecurity Incident Review Mechanism, the Regulation institutionalizes coordinated operational governance across all stages of cybersecurity incidents.[425] In doing so, cybersecurity increasingly shifts from a predominantly national regulatory competence toward a shared resilience responsibility embedded within a supranational governance architecture.

At the preventive and preparedness stages, the Regulation establishes a permanent infrastructure for systemic resilience through the integration of National Cyber Hubs, Cross-Border Cyber Hubs, CSIRTs, ENISA, and EU-CyCLONe into a coordinated information-sharing ecosystem.[426] Legally, this reflects an evolution from the risk-management logic of the NIS2 Directive toward a model based on continuous operational awareness and anticipatory governance.

---

[424] VILLANI, 2025, p.497.
[425] European Parliament and Council of the European Union, Regulation (EU) 2025/38 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act), Articles (10,14,21)
[426] VILLANI, 2025, p.490.

The Act embeds interoperability obligations, structured intelligence exchanges, coordinated preparedness testing and Union-funded technological capabilities into the cybersecurity lifecycle, thereby reducing regulatory fragmentation between Member States.

The Act further deepens lifecycle-based governance by institutionalizing solidarity during and after cyber incidents. It embeds cybersecurity within a broader framework of operational solidarity, coordinated accountability, and continuous resilience enhancement across Member States.

In this context, the EU Cybersecurity Reserve transforms mutual assistance from a largely political commitment into an operationalized support mechanism capable of facilitating coordinated response and recovery during large-scale cyber incidents. Simultaneously, the European Cybersecurity Incident Review Mechanism introduces an institutionalized process of post-incident evaluation designed to identify structural weaknesses, assess response effectiveness, and generate lessons for future risk mitigation.[427] Compared with earlier European instruments focused primarily on prevention and notification, the Cyber Solidarity Act reflects a significantly more mature and systemically integrated model of cybersecurity governance.

Nevertheless, the European model also reveals structural tensions inherent within highly integrated supranational frameworks. The operationalization of cyber solidarity raises challenges concerning national sovereignty sensitivities, coordination complexity among multiple institutional actors, reliance on private cybersecurity providers, and the management of cross-border information sharing in areas closely connected to national security interests. Consequently, while the Cyber Solidarity Act strengthens collective cyber resilience, it illustrates the legal and institutional complexities associated with constructing operationally integrated transnational systems.

By contrast, the Jordanian cybersecurity framework has not yet institutionalized comparable mechanisms of operational solidarity or integrated systemic resilience governance within a binding legal structure. While Jordan—as a unitary state—does not require supranational mechanisms equivalent to the EU model, its domestic functional equivalent structured, cross-

[427] European Parliament and Council of the European Union, Regulation (EU) 2025/38 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act), Article 21.

sectoral mutual assistance, integrated emergency capabilities, and statutory incident review mechanisms remains comparatively underdeveloped. Although the NCSC and the JoCERT perform an important coordinating role in incident response and national cybersecurity oversight, their functions continue to operate primarily through administrative coordination and policy implementation, rather than through legally codified cross-sectoral mutual aid obligations or formalized post-incident inquiry mandates.[428]

At the same time, Jordan's current cybersecurity strategy reflects an evolving governance model in which institutional capacity-building and policy development precede the establishment of fully enforceable resilience structures.[429] Existing national mechanisms demonstrate an increasing recognition of cybersecurity resilience as a strategic priority, particularly through growing emphasis on administrative coordination, national preparedness, and inter-agency cooperation. However, the absence of integrated recovery coordination systems, structured cross-sectoral interoperability mechanisms, and formalized post-incident learning frameworks continues to constrain the operational maturity of the Jordanian resilience architecture.

Measured against the evaluative criteria of the Regulatory Maturity Matrix, the divergence between the EU and Jordan extends beyond differences in discrete statutory provisions, reflecting fundamentally distinct governance architectures. Whereas the EU adopts a distributed and operationally integrated resilience model characterized by supranational solidarity and institutionalized post-incident review—classifying it as high maturity—the Jordanian framework remains primarily grounded in centralized administrative oversight and state-led incident response mechanisms.[430]

By contrast, the Jordanian framework lacks codified inter-sectoral mutual aid obligations, automated threat-sharing channels, and statutory recovery frameworks. Consequently, Jordan falls within the low maturity tier for cyber solidarity and systemic resilience governance, reflecting a

[428] National Cybersecurity Center, National Plan for Combating Cyber Threats, available at https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/national_plan_for_combating_cyber_threats-0.pdf, (Accessed 14 May 2026).
[429] National Cybersecurity Center, Jordan National Cybersecurity Framework Capabilities, available at https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/jordan_national_cybersecurity_framework_capabilities.pdf, (Accessed 14 May 2026).
[430] ALMOMANI et al., 2026, p.30.

structure that cannot yet operationalize a continuous, lifecycle-based resilience cycle equivalent to the European model.

V.7 General Comparative Findings

While both legal orders formally recognize cybersecurity as a strategic sovereign imperative, the analysis reveals profound variations in the degree of legal bindingness, institutional distribution, and regulatory maturity characterizing their respective systems. Methodologically, these maturity classifications are determined based on the cumulative presence or absence of legally binding obligations, the degree of statutory specificity, risk differentiation, institutional specialization, enforceability, private-sector allocation of responsibilities, lifecycle coverage, and structural mechanisms for coordination and resilience.

By evaluating both frameworks through the eight dimensions of the Regulatory Maturity Matrix using these criteria, this synthesis systematically resolves the four core research questions established at the outset of the comparative inquiry, bridging doctrinal statutory analysis with functional governance outcomes.

In answering the first comparative question concerning the specific legal and institutional mechanisms enacted, the analysis reveals fundamentally distinct statutory foundations. The EU has constructed a comprehensive, multi-layered regulatory corpus dominated by directly applicable regulations and harmonized directives, principally the NIS2 Directive, the GDPR, the CRA, and the Cyber Solidarity Act.

Together, these instruments establish an interconnected statutory web regulating organizational risk management, horizontal product security, data protection, and collective emergency response. Conversely, the Jordanian architecture remains anchored in a centralized primary statute, Cybersecurity Law No. 16 of 2019, complemented by the PDPL No. 24 of 2023. Rather than promulgating dense primary statutory mandates for each governance phase, the Jordanian model relies on the NCSC to issue secondary executive instructions, administrative policies, and technical guidelines and national strategies.

In evaluating the second inquiry regarding how these mechanisms operate in practice and the precise legal duties they generate, the comparison demonstrates contrasting operational methodologies. Within the EU, statutory duties are legally enforceable, proactive, and temporally

continuous. Under Article 21 of the NIS2 Directive and Article 32 of the GDPR, covered entities must implement technical and organizational measures calibrated to dynamic risk environments, while Annex I of the CRA imposes mandatory security-by-design requirements and continuous vulnerability handling across the product lifespan. Furthermore, reactive and post-incident mechanisms under Articles 23 and 34 of NIS2 generate strict, phased reporting obligations timelines backed by significant administrative financial penalties.

In contrast, the Jordanian framework operates primarily through centralized administrative supervision and organizational self-assessment. While primary legislation mandates general compliance and incident reporting under Article 6 of Law No. 16 of 2019, operational response timelines, severity tiers, and post-incident recovery procedures remain articulated in administrative policies that lack primary statutory penalties and formal verification procedures.

Regarding the third inquiry concerning structural divergences, the application of the Regulatory Maturity Matrix confirms that the divide between the two systems reflects fundamentally opposing governance philosophies and institutional designs. The EU model embodies a distributed governance architecture that systematically disperses cybersecurity responsibilities across public supervisory authorities, national CSIRTs, supranational bodies like ENISA and EU-CyCLONe, software manufacturers, and commercial supply chains. This model integrates risk proportionality as a mandatory statutory constraint, legally differentiating compliance obligations based on entity size, sector criticality, and threat severity.

In stark contrast, the Jordanian framework embodies a state-centric, command-and-control governance philosophy. Regulatory authority, threat monitoring, investigative powers, and administrative sanctioning remain concentrated almost exclusively within the NCSC, resulting in uniform statutory mandates that lack codified risk-tiering benchmarks, independent supervisory specialization, and structured judicial oversight mechanisms.

These structural variations produce distinct operational consequences for systemic cybersecurity resilience, thereby resolving the fourth comparative research inquiry. The EU's distributed, lifecycle-oriented model achieves high operational interoperability, granular threat visibility, and systemic cross-border coordination. However, the comparative analysis critically reveals that high regulatory maturity generates substantial operational and economic burdens.

The coexistence of overlapping legal instruments (NIS2, CRA, GDPR) creates interpretative ambiguity and duplicative reporting duties, while the cumulative costs of conformity assessments, technical documentation, and sustained vulnerability management impose severe financial strain on economic operators, particularly SMEs.[431] Moreover, the CRA's requirement for long-term security support creates a precarious structural dependency on the commercial longevity of manufacturers, introducing systemic vulnerabilities if market actors discontinue operations or leave products orphaned without patches

Conversely, Jordan's centralized, executive-driven model provides distinct functional advantages in immediate command-and-control agility, enabling rapid administrative decisions and national security mobilization during acute cyber crises. However, the absence of legally codified lifecycle obligations, standardized statutory incident thresholds, and mandatory post-incident audit requirements produces operational inconsistency and compliance uncertainty across critical sectors.

The EU should therefore not be understood simply as "better"; rather, it represents a different regulatory equilibrium among legal bindingness, risk calibration, institutional complexity, resilience, and economic burden. Jordan occupies a different position on this regulatory spectrum, reflecting a more centralized and comparatively less complex regulatory architecture whose advantages and limitations must be assessed in light of its institutional and economic context.

Accordingly, this chapter demonstrates that regulatory maturity cannot be measured purely by the formal volume of legislation, but depends upon the dynamic equilibrium among statutory bindingness, institutional capacity, risk proportionality, operational interoperability, and continuous resilience integration. While the EU reflects a highly integrated model of lifecycle governance, its sophisticated structures demand substantial institutional capital, technical infrastructure, and market absorption capabilities. The Jordanian framework, while structurally adaptable and strategically ambitious under the National Cybersecurity Strategy 2025–2028, remains in a transitional phase characterized by a persistent gap between strategic policy

[431] RISWALDI, 2025, p.347.

aspirations and enforceable statutory codification. The overarching comparative findings across both jurisdictions are synthesized in Table 1 below.

Dimension	**EU**	**Jordan**	**Comparative finding**
Legal bindingness	High	Medium	EU obligations are more extensively codified and enforceable.
Risk proportionality	High	Medium	EU provides more differentiated risk-based obligations.
Enforcement mechanisms	High	Medium	EU has more structured and multi-level enforcement.
Institutional capacity	High / Distributed	Centralized / Developing	Different institutional models, with stronger EU specialization.
Private-sector engagement	High	Medium	EU allocates broader and more differentiated duties to private actors.
Lifecycle continuity	High	Nascent / Low	EU integrates prevention, response, recovery, and vulnerability management more extensively.

Dimension	EU	Jordan	Comparative finding
Resilience integration	High	Nascent / Low	EU more strongly embeds systemic and collective resilience.
Operational interoperability	High	Medium	EU provides stronger cross-border and multi-institutional coordination.

Table 1: - Comparative Findings across the Eight Dimensions of the Regulatory Maturity Matrix

These comparative findings lead to a critical doctrinal conclusion regarding legal transferability: the direct transplantation of complex EU cybersecurity regulations into Jordan is neither legally feasible nor economically desirable. Introducing high-intensity certification regimes, prescriptive lifecycle obligations, and complex multi-tiered reporting structures without the requisite institutional infrastructure, technical accreditation bodies, and private-sector capital would disproportionately burden Jordanian SMEs, stifle digital innovation, and generate widespread implementation deficits.

Rather, effective regulatory development in Jordan requires a context-sensitive, gradual approach that strengthens primary statutory bindingness, introduces proportional risk tiering, and formalizes institutional oversight in alignment with domestic economic and administrative capacities. Building upon this comprehensive comparative diagnosis, the following chapter transitions from normative and structural comparison to examine the practical implementation of the EU cybersecurity regulation across selected Member States. Through that empirical and operational inquiry, the study identifies implementation challenges, administrative bottlenecks, and best practices to construct the evidentiary foundation for the contextualized reform roadmap developed subsequently in Chapter VII.

Chapter VI: Practical Implementation of Cybersecurity Governance in Selected EU Member States: Implications for Jordan

VI.1 Transition from Comparative Assessment to Practical Implementation

The preceding chapter examined the cybersecurity governance frameworks of the EU and Jordan through a structured comparative analysis grounded in the Regulatory Maturity Matrix. That assessment demonstrated significant divergences between the two systems in relation to legal bindingness, institutional capacity, risk proportionality, lifecycle continuity, operational interoperability, and resilience-oriented governance. While the EU has progressively developed an integrated and highly institutionalized cybersecurity governance architecture, the Jordanian framework remains comparatively centralized and policy-oriented, operating within more limited institutional and operational capacities.

However, a comparative analysis of formal legal frameworks alone does not fully capture the practical effectiveness of cybersecurity governance. The existence of advanced legal instruments does not necessarily guarantee uniform implementation, operational coherence, or effective cybersecurity outcomes. In practice, the implementation of cybersecurity legislation is shaped by a wide range of institutional, technical, economic, and political factors that influence how legal obligations are interpreted, operationalized, and enforced within different national contexts.

Although the EU cybersecurity legislation seeks to promote harmonization across Member States, practical implementation remains uneven due to differences in administrative structures, supervisory capacities, technical expertise, economic resources, and national cybersecurity priorities. Consequently, the implementation of instruments such as the NIS2 Directive,[432] the GDPR,[433] the CRA,[434] and the Cyber Solidarity Act[435] has generated varying operational models

[432] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive).
[433] European Parliament and Council of the European Union, Regulation No. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
[434] European Parliament and Council of the European Union, Regulation No. 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act).
[435] European Parliament and Council of the European Union, Regulation (EU) 2025/38 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act).

across Member States, resulting in institutional diversity and divergent regulatory practices, some of which may give rise to fragmentation.

The chapter proceeds from the premise that cybersecurity governance effectiveness is determined not solely by the sophistication of legal instruments, but by the extent to which regulatory obligations are translated into operational capabilities, institutional coordination, and adaptive resilience mechanisms.

Recent scholarship has further emphasized that the effective harmonization of EU cybersecurity governance depends not merely upon the adoption of formal legislation, but also upon implementation practices, institutional cooperation, and the integration of regulatory and technical frameworks across Member States.[436]

In this regard, cybersecurity governance increasingly operates through a dual structure that combines technical coordination mechanisms with broader resilience objectives relating to the protection of fundamental rights, critical infrastructures, and the integrity of the shared digital space. This development reflects a broader transformation from isolated compliance-based approaches toward integrated, resilience-oriented, and system-based governance models.

At the same time, these implementation divergences provide valuable comparative insights. The diversity of approaches adopted across Member States demonstrates that effective cybersecurity governance cannot be reduced to a single regulatory model or achieved solely through legislative sophistication. Rather, governance effectiveness depends upon the interaction between legal obligations, institutional coordination, operational interoperability, technical capacity, and broader resilience infrastructures.[437] In this respect, implementation diversity within the EU simultaneously represents both a governance challenge and a source of practical lessons for jurisdictions seeking to strengthen their cybersecurity frameworks.

Against this background, the present chapter moves beyond normative and doctrinal comparison toward an examination of the practical implementation of EU cybersecurity legislation

[436] Casarosa, Federica – Comandé, Giovanni, Implementing the NIS 2 Directive: Towards Harmonisation or Further Fragmentation? In: Joint National Conference on Cybersecurity (ITASEC & SERICS 2026), Cagliari, Italy, 9–13 February 2026. CEUR Workshop Proceedings, 2026. Available at: https://ceur-ws.org/Vol-4198/paper19.pdf (Accessed 24 May 2026).
[437] COTTA – RIGHETTINI, 2026, p.3.

and the operational challenges arising from fragmented implementation across Member States. The chapter further examines how regional cooperation mechanisms within the EU seek to mitigate fragmentation through supranational coordination, operational interoperability, and collective resilience structures.

Ultimately, the chapter aims to assess how the practical experiences of EU Member States may provide context-sensitive implications for the future development of cybersecurity governance in Jordan. EU cybersecurity harmonization therefore produces convergence at the level of regulatory objectives and minimum substantive requirements, but does not eliminate divergence in institutional design, supervisory practice, verification mechanisms, or operational implementation. Rather than advocating the direct transplantation of EU regulatory models, the analysis seeks to identify broader governance approaches relating to institutional coordination, phased implementation, and operational integration that may contribute to the gradual strengthening of cybersecurity resilience in Jordan.

VI.2 Diversity in the Implementation of EU Cybersecurity Legislation

Although EU cybersecurity legislation establishes increasingly common regulatory objectives, implementation divergence persists across several operational dimensions. Fragmentation is particularly evident in the organization of supervisory authorities, the allocation of enforcement responsibilities, the development of incident reporting infrastructures, the implementation of risk management requirements, and the integration of cybersecurity certification mechanisms. Consequently, Member States frequently operationalize identical legal obligations through differing institutional arrangements, administrative practices, and governance structures.

France, Germany, and Hungary provide useful examples of differing cybersecurity governance approaches within the EU and are therefore selected for comparative examination. These Member States were selected due to their contrasting institutional structures, administrative traditions, and levels of operational coordination.[438] France is examined as a case of institutional preparedness and ongoing NIS2 transposition. It reflects a comparatively centralized cybersecurity governance model characterized by strong national coordination, whereas Germany represents a more decentralized and federal implementation structure involving multiple supervisory

[438] SCHMITZ-BERNDT – CHIARA, 2022, p.307.

authorities.[439] Hungary, by contrast, was selected as the first EU Member State to formally complete the transposition and application of the NIS2 Directive, providing critical insight into the implementation challenges and governance dynamics of operating within a centralized, regulatory-driven environment.[440] Together, these examples provide a useful comparative basis for examining the practical fragmentation of EU cybersecurity implementation across different regulatory and institutional contexts.

VI.2.1 Diversity in National Transposition and Regulatory Approaches

One of the clearest manifestations of implementation fragmentation within EU cybersecurity governance can be observed in the national transposition of the NIS2 Directive. While the NIS2 Directive establishes a harmonized baseline of substantive minimum requirements across the Union, it preserves significant national discretion regarding institutional organization, supervisory design, and specific implementation techniques. As a result, the operationalization of cybersecurity obligations continues to be influenced by national administrative structures, regulatory traditions, and institutional capacities.

Nevertheless, the NIS2 Directive reflects a broader legislative effort to reduce fragmentation and limit excessive national discretion through the introduction of more objective and harmonized criteria for identifying essential and important entities, thereby narrowing the scope of divergent national implementation approaches.[441] Consequently, the practical application of EU cybersecurity obligations frequently diverges across designated national legal systems, producing varying models of cybersecurity governance despite the existence of a shared supranational regulatory framework.

The German transposition process was formalized through the adoption of *the NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz* (NIS2 Implementation and Cybersecurity Strengthening Act), which amended the Federal Office for Information Security Act *(Bundesamt für Sicherheit in der Informationstechnik-Gesetz – BSIG*) and significantly expanded the supervisory and enforcement powers of the Federal Office for Information Security *(Bundesamt*

[439] SAŁEK – FAJDEK, 2025, p.44.
[440] Casarosa, Federica – Comandé, Giovanni, Implementing the NIS 2 Directive: Towards Harmonisation or Further Fragmentation? In: Joint National Conference on Cybersecurity (ITASEC & SERICS 2026), Cagliari, Italy, 9–13 February 2026. CEUR Workshop Proceedings, 2026. Available at: https://ceur-ws.org/Vol-4198/paper19.pdf (Accessed 25 May 2026).
[441] Ibid.

für Sicherheit in der Informationstechnik – BSI), particularly through §§ 59–63 BSIG, which establish its supervisory competence and provide for supervisory and enforcement measures in relation to particularly important and important entities.[442]

Although Article 41(1) of the NIS2 Directive required Member States to adopt and publish the necessary transposition measures by 17 October 2024,[443] the German implementation process experienced delays. The Act was promulgated on 5 December 2025 and entered into force on 6 December 2025.[444] Consequently, Germany completed its principal legislative transposition more than one year after the deadline established by Article 41 of the NIS2 Directive.

The French transposition process has primarily been pursued through *the Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité* (Draft Law on the Resilience of Critical Infrastructure and the Strengthening of Cybersecurity), which is intended to transpose the NIS2 Directive, alongside the CER and DORA frameworks, into French law. The draft law was adopted by the French Senate at first reading on 12 March 2025 and transmitted to the National Assembly for further consideration.[445] Accordingly, the French case should not be characterized as a completed NIS2 transposition; rather, it represents an implementation process that remained institutionally and legislatively in transition.

Nevertheless, the absence of completed legislative transposition should not be equated with an absence of implementation capacity. France entered the NIS2 process with an already developed institutional cybersecurity architecture, centered particularly on *the Agence nationale de la sécurité des systèmes d'information* (ANSSI).[446] This institutional framework had established significant capabilities in cybersecurity governance, critical infrastructure protection, incident response, technical support, and regulatory coordination before the completion of the NIS2

---

[442] Germany, *Bundesamt für Sicherheit in der Informationstechnik-Gesetz* (BSIG) as amended by the *NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz* (2025), *Bundesgesetzblatt* [BGBl] I, 2 December 2025, No. 301, p. 2. Available at: https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html. (Accessed 26 September 2026).

[443] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 41(1).

[444] Germany, *Bundesamt für Sicherheit in der Informationstechnik-Gesetz* (BSIG) as amended by the *NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz* (2025).

[445] France, Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (Projet de loi n° 33, Sénat, 15 October 2024), https://www.senat.fr/leg/tas24-078.html (Accessed 31 May 2026).

[446] France, Agence nationale de la sécurité des systèmes d'information (ANSSI), The NIS 2 Directive. Available at https://cyber.gouv.fr/en/regulations/the-nis-2-directive/, (Accessed 31 May 2026).

transposition process. ANSSI has also been preparing entities for the forthcoming NIS2 regime through guidance, eligibility tools, and support mechanisms.

The French case therefore illustrates an important distinction between formal regulatory transposition and institutional preparedness. While the former remained incomplete during the period examined, the latter was comparatively advanced. France may consequently be understood as a case of implementation in transition, in which pre-existing institutional and operational capacities preceded the completion of the NIS2 legislative framework.

Hungary initially introduced NIS2-related requirements through Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision which introduced the initial elements of the national cybersecurity framework, including certification, supervision, and registration requirements for regulated entities.[447] The framework was subsequently consolidated and replaced by Act LXIX of 2024 on the Cybersecurity of Hungary, and Government Decree 418/2024 (XII.),[448] the act entered into force on 1 January 2025 and currently provides a comprehensive transposition for Hungary's cybersecurity framework.[449]

Unlike jurisdictions that experienced prolonged legislative delays, Hungary pursued an incremental transposition process that aligned national cybersecurity obligations with the NIS2 requirements. The Hungarian model is comparatively centralized, with substantial supervisory functions assigned to the Supervisory Authority for Regulated Activities (SZTFH), alongside other designated cybersecurity institutions, national CSIRT functions, and specialized competent authorities exercising regulatory oversight over compliance, certification, and incident reporting.[450]

The comparison illustrates that implementation fragmentation does not arise solely from differences in legal obligations, but also from variations in administrative capacity, legislative

[447] Hungary, Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision. Available https://njt.jog.gov.hu/jogszabaly/en/2023-23-00-00?utm, (Accessed 31 May 2026).
[448] Hungary, Government Decree 418/2024 (23 December 2024) on the Implementation of the Act on the Cybersecurity of Hungary, National Legislation Database *(Nemzeti Jogszabálytár),* available at: https://njt.hu/jogszabaly/2024-418-20-22.7 (Accessed 28 September 2026).
[449] Hungary, Act LXIX of 2024 on the Cybersecurity of Hungary. Available at https://njt.hu/jogszabaly/en/2024-69-00-00 (Accessed 31 May 2026).
[450] Hungary, the Supervisory Authority for Regulated Activities. Available at https://sztfh.hu/ugyintezes/nyomtatvanyok-es-urlapok/sztfh420/. (Accessed 31 May 2026).

priorities, and institutional preparedness. France's pre-existing cybersecurity infrastructure enabled substantial operational alignment with NIS2 objectives despite delayed formal transposition.

Germany's federal governance structure contributed to a more complex implementation process requiring coordination among multiple authorities. Hungary, by contrast, adopted a more centralized legislative approach that facilitated earlier transposition through concentrated supervisory authority. These differences demonstrate how national governance structures continue to shape the practical implementation of harmonized EU cybersecurity obligations despite the existence of a common Union regulatory framework.

VI.2.2 Diversity in Risk Management and Compliance Obligations

Risk-management and compliance obligations provide one of the clearest examples of how harmonized EU cybersecurity requirements are operationalized differently across Member States. Although Article 21 of NIS2 establishes a common substantive framework for cybersecurity risk-management measures, Member States retain significant discretion concerning institutional arrangements, supervisory procedures, verification mechanisms, and certain implementation techniques.[451] As a result, significant differences have emerged in relation to risk-assessment methodologies, compliance-monitoring mechanisms, audit requirements, supervisory practices, and the degree of regulatory prescriptiveness, demonstrating how national regulatory traditions and institutional capacities continue to shape cybersecurity governance.

Germany has adopted a structured and compliance-oriented approach to cybersecurity risk management. Central to this framework is § 30 BSIG, which requires essential and important entities to implement “appropriate, proportionate and effective technical and organizational measures” to manage risks affecting the security of network and information systems.[452] The provision largely mirrors Article 21 of the NIS2 Directive but further embeds these obligations within Germany’s broader supervisory architecture under the BSI.

The framework incorporates risk analysis, information security policies, incident handling, business continuity planning, supply-chain security, vulnerability management, access controls, encryption, and cybersecurity awareness measures within a continuous risk-management cycle.

[451] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 21.
[452] Germany, Bundesamt für Sicherheit in der Informationstechnik-Gesetz (BSIG), § 30.

Compliance is reinforced through the extensive supervisory powers of the BSI, including the authority to issue technical guidance, monitor compliance, and request information from regulated entities.

In France, cybersecurity risk management is operationalized through a multi-tiered governance structure that integrates primary statutory duties with administrative-technical frameworks. Rather than relying exclusively on abstract statutory mandates, the French framework translates overarching risk-management obligations into actionable security measures through specialized administrative instruments and technical tooling developed by ANSSI, such as the EBIOS Risk Manager methodology.[453]

This approach is embodied in the Cyber France Reference Framework *(Référentiel d'exigences Cyber France – ReCyF)*,[454] which does not replace primary legislation, but operates as an administrative-technical implementation framework and compliance benchmark, [455] *ReCyF* establishes standardized specifications covering governance arrangements, asset management, access controls, security monitoring, incident response, and business continuity. A defining feature of this approach is its treatment of risk management as an ongoing governance process rather than a static legal formality, reinforced through centralized ANSSI oversight, security assessments, technical inspections, and continuous incident monitoring.

Hungary has adopted a prescriptive approach to cybersecurity risk management. Under Chapter III of Act LXIX of 2024 on the Cybersecurity of Hungary, regulated entities are required to implement technical, organizational, and operational security measures proportionate to the risks affecting their electronic information systems and classify those systems according to predefined security categories based on confidentiality, integrity, and availability requirements.[456] Rather than relying on flexible, principles-based standards, this granular requirement illustrates

[453] France, Agence nationale de la sécurité des systèmes d'information (ANSSI). The EBIOS Risk Manager Method: Reference tool for digital risk analysis and management. Available at: https://cyber.gouv.fr/la-methode-ebios-risk-manager (Accessed 3 June 2026).
[454] France, Agence nationale de la sécurité des systèmes d'information (ANSSI): ReCyF : publication du référentiel d'exigences et du comparateur accessibles sur MesServicesCyber, https://lab.cyber.gouv.fr/les-actualit%C3%A9s-du-lab-anssi/recyf--publication-du-r%C3%A9f%C3%A9rentiel-dexigences-et-du-comparateur/ (Accessed 1 June 2026).
[455] France, Agence nationale de la sécurité des systèmes d'information (ANSSI): NIS 2 – National Transposition Cybersecurity Risk Management Measures. ReCyF: France's Cyber Framework. Version 2.5 (Working Version), 2026. Available at https://messervices.cyber.gouv.fr/nis2#exigences, (Accessed 2 June 2026).
[456] Hungary, Act LXIX of 2024 on the Cybersecurity of Hungary, chapter III, https://njt.hu/jogszabaly/en/2024-69-00-00 (Accessed 31 May 2026).

how the Hungarian legislature translates broader EU risk-management mandates into an explicit, state-defined technical baseline.

A distinctive feature of the Hungarian model is the strong emphasis placed on regulatory verification. Compliance with risk-management obligations is reinforced through mandatory cybersecurity audits conducted by accredited audit organizations, extensive registration requirements, and continuous supervisory oversight exercised by the SZTFH. Consequently, the Hungarian framework reflects a formalized, compliance-driven approach that prioritizes *ex-ante* supervision, standardized security categorization, and regulatory accountability

While all three jurisdictions require regulated entities to adopt risk-based cybersecurity measures, they differ significantly in the legal techniques and institutional mechanisms through which these obligations are operationalized. Germany provides a comparatively codified, highly enforceable framework supported by a specialized supervisory authority,[457] although the degree of legal formalization may reduce operational flexibility and increase compliance costs.[458] France offers an adaptive and operationally oriented model based on technical guidance and centralized institutional expertise. Hungary occupies an intermediate position, combining centralized oversight with extensive external audit and verification requirements that strengthen accountability while potentially increasing administrative burdens for regulated entities.

This comparison further illustrates that implementation fragmentation within the EU extends beyond legislative transposition to encompass the practical organization of cybersecurity governance itself. While Member States broadly pursue the same regulatory objectives under the NIS2 Directive, they differ significantly in the mechanisms through which cybersecurity risks are assessed, supervised, and verified. These variations reflect differing national approaches to legal bindingness, institutional capacity, enforceability, and operational implementation, demonstrating that regulatory effectiveness depends not only on the substantive content of legal obligations but also on the institutional governance structures through which they are implemented, monitored, and enforced.[459]

[457] Germany, Bundesamt für Sicherheit in der Informationstechnik-Gesetz (BSIG), § 30.
[458] TEICHMANN, 2025, p.211.
[459] Ibid., p.215.

For Jordan, these implementation experiences demonstrate that effective cybersecurity risk governance requires more than formal adoption of legal obligations. The German, French, and Hungarian experiences collectively highlight the importance of aligning risk-management requirements with appropriate supervisory mechanisms, technical guidance, and compliance-verification structures. More broadly, they illustrate how different governance models may achieve similar cybersecurity objectives while reflecting distinct institutional capacities and regulatory traditions.

VI.2.3 Diversity in Incident Reporting Obligations and Notification Frameworks

The NIS2 Directive significantly expands and harmonizes incident-reporting obligations by establishing common requirements for essential and important entities. Article 23 establishes a staged reporting framework requiring an early warning without undue delay and in any event within 24 hours of becoming aware of a significant incident, an incident notification within 72 hours, and a final report within one month.[460] This staged model is intended to ensure timely information exchange between regulated entities and competent authorities and to enhance coordinated incident management across the Union.[461]

Despite these harmonization objectives, incident-reporting obligations continue to exhibit notable fragmentation across Member States, particularly in relation to reporting thresholds, incident classification systems, notification procedures, and supervisory arrangements.[462] These differences reflect varying national approaches to legislative design, regulatory supervision, and operational implementation.

Germany has adopted a strictly codified approach to cybersecurity incident reporting through § 32 BSIG, which closely mirrors the reporting architecture established by Article 23 of the NIS2 Directive. The provision requires particularly important entities *(besonders wichtige Einrichtungen)* and important entities *(wichtige Einrichtungen)* to report significant security incidents *(erhebliche Sicherheitsvorfälle)* through a centralized reporting mechanism jointly

[460] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 23.
[461] Casarosa, Federica – Comandé, Giovanni, Implementing the NIS 2 Directive: Towards Harmonisation or Further Fragmentation? In: Joint National Conference on Cybersecurity (ITASEC & SERICS 2026), Cagliari, Italy, 9–13 February 2026. CEUR Workshop Proceedings, 2026. Available at: https://ceur-ws.org/Vol-4198/paper19.pdf (Accessed 25 May 2026).
[462] SAŁEK – FAJDEK, 2026, p.47.

operated by the Federal Office for Information Security (BSI) and the Federal Office of Civil Protection and Disaster Assistance (BBK).[463]

Regulated entities must submit: (1) an early warning within 24 hours of becoming aware of a significant security incident; (2) an incident notification within 72 hours containing an initial assessment of the incident's severity and impact; (3) intermediate reports upon request by the BSI; and (4) a final report within one month describing the incident, its causes, remedial measures, and any cross-border effects.[464] Unlike implementation models that rely primarily on administrative guidance, Germany embeds both the substantive reporting obligations and the procedural reporting stages directly within the primary legislation, thereby providing a high degree of legal certainty, procedural clarity, and regulatory enforceability.

Germany has also established a relatively detailed incident-classification framework. Section 2(11) BSIG defines a "significant security incident" *(erheblicher Sicherheitsvorfall)* as an incident that causes or is capable of causing serious operational disruption, significant financial losses, or substantial material or non-material harm to affected persons.[465] This definition links reporting obligations to predefined legal thresholds and reduces uncertainty concerning when notification duties are triggered. The framework further recognizes related categories such as cyber threats *(Cyberbedrohungen),* significant cyber threats *(erhebliche Cyberbedrohungen)*, security incidents *(Sicherheitsvorfälle)*, and near misses (Beinahevorfälle), thereby creating a comparatively structured legal classification framework for incident assessment and reporting.[466]

The notification procedure is reinforced through a centralized supervisory architecture under the BSI. Beyond receiving incident reports, the BSI functions as the national contact point, central reporting authority, and coordinating body for cross-border incident cooperation. Where a significant incident affects multiple Member States, the BSI is responsible for notifying the affected Member States and ENISA while ensuring the protection of confidential information and economic interests.[467]

[463] Germany, Bundesamt für Sicherheit in der Informationstechnik-Gesetz (BSIG), § 32.
[464] Ibid.
[465] Ibid., § 2(11).
[466] Ibid., §2(1), §2(6), §2(10), §2(11), §2(40).
[467] Ibid., §32(4)(3).

In France, the operationalization of incident-reporting obligations reflects a distinct model where administrative preparedness precedes completed statutory transposition. While the formal legislative transposition of Article 23 of the NIS2 Directive is being finalized through *the Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité*,[468] France has structured its incident-notification framework around the operational coordination channels of ANSSI.

France has progressively developed incident-reporting procedures that are being aligned with the three-stage notification framework established by Article 23 of the NIS2 Directive.[469] Regulated entities are required to submit an initial early warning within 24 hours of becoming aware of a significant incident, followed by an incident notification within 72 hours and a final report within one month.[470] Unlike the German framework, where these reporting stages are expressly codified within the BSIG, the French approach relies on a combination of the ongoing NIS2 transposition process, existing cybersecurity regulations, and operational procedures coordinated by ANSSI. Consequently, reporting obligations are implemented through a more operationally driven framework rather than through a single comprehensive statutory provision.

With respect to incident classification, the French approach places significant emphasis on the practical consequences of cybersecurity incidents, particularly their impact on service continuity and the functioning of essential services.[471] Rather than establishing a detailed statutory taxonomy of reportable incidents, the French framework evaluates incident significance through impact-based criteria that closely reflect the risk-based approach adopted by Article 23 of the NIS2 Directive.[472] This provides greater flexibility in incident assessment but may also leave a broader margin for supervisory interpretation.

---

[468] France, Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, Dossier législatif, Sénat, available at: French Senate legislative dossier (Accessed 28 September 2026).

[469] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 23.

[470] France, Agence nationale de la sécurité des systèmes d'information (ANSSI): NIS 2 – National Transposition Cybersecurity Risk Management Measures. ReCyF: France's Cyber Framework. Version 2.5 (Working Version), 2026. Available at https://messervices.cyber.gouv.fr/nis2#exigences, (Accessed 30 June 2026).

[471] France, Agence nationale de la sécurité des systèmes d'information (ANSSI), *OSE – Déclaration d'incident*, available at: https://cyber.gouv.fr/contact-acces/contact/notifications-reglementaires/?utm (Accessed 28 September 2026).

[472] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 23.

The notification procedure is organized through centralized reporting channels coordinated by ANSSI, enabling incident information to be consolidated, assessed, and disseminated where necessary. Following notification, reporting entities may be required to provide supplementary information regarding the nature of the incident, mitigation measures, and recovery activities.[473] In addition, incident reports contribute to broader situational awareness and coordination activities at both the national and European levels.

In Hungary, the central incident notification framework is established under Section 66 of Act LXIX of 2024. While the Hungarian regulatory taxonomy establishes a broad conceptual framework covering various tiers of cyber threats and incidents, the operative reporting obligations under Section 66 specifically mandate the notification of significant cybersecurity incidents affecting essential and important services.[474]

Unlike implementation models that focus exclusively on significant incidents, the Hungarian framework adopts a broader reporting architecture encompassing cyber threats, cybersecurity near misses, cybersecurity incidents, and operational cybersecurity incidents. The legislation further differentiates reporting obligations according to the nature and impact of the incident, requiring the reporting of events that cause serious service disruption, financial losses, or significant material or non-material harm.[475]

In this regard, the Act provides a detailed statutory definition of a "significant cybersecurity incident," thereby linking reporting obligations to predefined legal criteria and enhancing legal certainty for regulated entities.[476] This contrasts with implementation approaches that rely more closely on the general significance criteria established under the NIS2 Directive.

A distinctive feature of the Hungarian model concerns its legislative technique for implementing incident-reporting obligations. While Hungary ultimately seeks to achieve compliance with the reporting architecture envisaged under Article 23 of the NIS2 Directive, the primary legislation does not codify the Directive's staged notification framework in the same

[473] France, Agence nationale de la sécurité des systèmes d'information, *Notifications réglementaires*, available at: https://cyber.gouv.fr/contact-acces/contact/notifications-reglementaires/ (Accessed 28 September 2026).
[474] Hungary, Act LXIX of 2024 on the Cybersecurity of Hungary. Section 66. Available at https://njt.jog.gov.hu/jogszabaly/en/2024-69-00-00 (Accessed 30 June 2026).
[475] Ibid.
[476] Ibid., Section 4, Article 40.

explicit manner as the German BSIG. Instead, Act LXIX of 2024 establishes the substantive duty to report cybersecurity incidents and defines the categories of reportable events, while important procedural requirements are distributed across implementing decrees and the broader supervisory framework administered by the competent authorities.[477]

From a comparative perspective, the implementation of incident-reporting obligations in Germany, France, and Hungary demonstrates that fragmentation persists despite the harmonizing objectives of the NIS2 Directive. Among these selected Member States, Germany provides the most explicit primary legislation codification of the reporting stages.[478] France, on the other hand, adopts a more operational model centered on supervisory coordination through ANSSI, while Hungary combines detailed statutory definitions of reportable incidents with a procedurally distributed framework supplemented by secondary regulation.

The comparison demonstrates that implementation divergence extends beyond reporting timelines and notification thresholds to encompass broader differences in legislative design, institutional coordination, and supervisory practice. Consequently, the effectiveness of incident reporting depends not only on formal reporting obligations but also on the clarity of reporting procedures, the precision of incident-classification systems, and the operational capacity of competent authorities.

The experiences of these Member States are relevant for Jordan insofar as they highlight the importance of linking incident classification systems to clearly defined reporting obligations and supervisory procedures. Jordan's principal gap is therefore not necessarily the absence of incident categories, but the limited legal linkage between classification, mandatory reporting triggers, escalation procedures, supervisory intervention, and post-incident accountability.

VI.2.4 Diversity in CRA-Based Conformity Assessment and Cybersecurity Assurance Mechanisms

A further dimension of national administrative implementation and institutional operationalization concerns governance structures established to support mandatory conformity assessment under the CRA, which introduced binding cybersecurity requirements for products with digital elements and requires manufacturers to demonstrate conformity before placing such products on the EU market.

[477] Ibid., Section 66(2).
[478] Germany, Bundesamt für Sicherheit in der Informationstechnik-Gesetz (BSIG), § 32.

Although the Regulation entered into force in late 2024, its obligations apply progressively, with provisions under Chapter IV (Articles 35–51) on the notification of conformity assessment bodies applying from 11 June 2026, and vulnerability reporting obligations are applying from 11 September 2026, and the remaining substantive obligations from 11 December 2027.[479]

Consequently, Member States must progressively adapt their administrative and technical apparatus to operationalize these mandates. The divergent institutional configurations emerging in Germany, Hungary, and France demonstrate that even a uniform, directly applicable EU Regulation is mediated through distinct national administrative structures.[480]

Germany entered the CRA implementation phase with substantial pre-existing technical and certification capacities within the BSI, while the national legal framework assigning CRA-specific market-surveillance and notification functions was still being established. Unlike Member States that are still developing the administrative infrastructure necessary for CRA implementation, Germany has integrated certification, conformity assessment, product-security evaluation, and market-surveillance functions within the BSI. The BSIG expressly empowers the BSI to develop criteria and procedures for conformity assessment, evaluate the security of information technology products, issue security certifications, act as the national cybersecurity certification authority, and verify conformity with technical security requirements.[481]

The German implementation approach integrates conformity assessment with technical standardization and lifecycle-oriented guidance. Through the BSI, Germany developed national technical guidelines—most notably Technical Guideline TR-03183—supporting manufacturers in operationalizing CRA requirements.[482] These initiatives support the practical operationalization of CRA requirements relating to security-by-design, vulnerability management, software transparency, coordinated vulnerability disclosure, and lifecycle security.

[479] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act).
[480] Ibid., Article 71.
[481] Germany, Bundesamt für Sicherheit in der Informationstechnik-Gesetz (BSIG), § 3.
[482] Germany, Federal Office for Information Security (BSI): Technical Guideline TR-03183-H – Cyber Resilience Requirements for Manufacturers and Products, available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-H_v1_1_0.pdf?__blob=publicationFile&v=2 (Accessed 4 July 2026).

Hungary has adopted a distinctly regulatory approach to the implementation of the CRA through Act CXXXV of 2025 on the Hungarian Implementation of the Cyber Resilience Regulation and the amendment of certain cybersecurity provisions.[483] Unlike Germany, where CRA implementation is largely integrated into the pre-existing technical and certification functions of the BSI, the Hungarian framework focuses primarily on establishing the legal and institutional mechanisms required for conformity assessment, notification, market-surveillance, and enforcement. The Act designates the SZTFH as both the notifying authority and the market-surveillance authority for the purposes of Regulation (EU) 2024/2847, thereby concentrating responsibility for CRA implementation within a single regulatory body.[484]

A particularly distinctive feature of the Hungarian model is the detailed regulation of conformity assessment bodies. Section 9 of Act CXXXV of 2025 inserts a comprehensive framework (Sections 80/C–80/F of the amended Act LXIX of 2024 on Cybersecurity) governing the registration, supervision, notification, monitoring, and reporting obligations of conformity assessment organizations and notified bodies.[485] The legislation requires conformity assessment bodies to satisfy the requirements of Article 39 of the CRA,[486] obtain registration with the SZTFH, comply with conflict-of-interest rules, participate in European cooperation mechanisms, submit annual reports, and remain subject to continuous supervisory oversight.[487]

The Act further creates a formal national registry of notified bodies and empowers the SZTFH to suspend or withdraw notifications where statutory requirements are no longer fulfilled. These provisions reflect a highly formalized compliance architecture centered upon administrative control and regulatory accountability rather than the technical-guidance model that characterizes German implementation.

---

[483] Hungary, Act CXXXV of 2025 on the Implementation of the European Union Cyber Resilience Regulation in Hungary and the Amendment of Certain Cybersecurity Provisions. Hungarian Gazette (Magyar Közlöny), No. 158, 29 December 2025. Available at https://magyarkozlony.hu/dokumentumok/adbf9bdb4753d3f6e020f3486f3a3e3ff734cb9e/megtekintes (Accessed 4 July 2026).
[484] Ibid., Section 9.
[485] Ibid.
[486] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), Article 39.
[487] Hungary, Act CXXXV of 2025 on the Implementation of the European Union Cyber Resilience Regulation in Hungary and the Amendment of Certain Cybersecurity Provisions, Chapter IX/A, Sections 80/C (registration), 80/D (conflict of interest), 80/E (registry and supervisory oversight), and 80/F (annual reporting and European cooperation).

The Hungarian approach also differs from Germany in relation to market-surveillance arrangements. Whereas the German BSIG relies heavily upon the technical expertise and product-security functions already exercised by the BSI, Hungary establishes an explicit CRA-specific market-surveillance regime.

Introduced via Section 9 of the 2025 Act (which inserts the market-surveillance framework under the newly added Sections 80/H and 80/I of the primary Cybersecurity Act), the SZTFH is granted general competence over CRA market-surveillance matters, supported by enforcement powers that include administrative sanctions and regulatory intervention against non-compliant products.[488] The legislation further introduces detailed procedural rules governing notifications, registration, supervisory reviews,[489] and administrative penalties,[490] thereby emphasizing legal control and procedural oversight as the principal instruments for ensuring CRA compliance.

France presents a distinct model of CRA implementation fragmentation, characterized by the distribution of conformity assessment, notification, accreditation, vulnerability-reporting, and market-surveillance functions across several institutional actors. Unlike Germany, where the BSI combines extensive technical certification, conformity assessment, and cybersecurity-standardization functions within a single specialized authority, and unlike Hungary, where Act CXXXV of 2025 designates SZTFH as both notifying authority and market-surveillance authority, the French model appears to rely on a more functionally differentiated institutional architecture.

Under the emerging French implementation framework for the Cyber Resilience Act, COFRAC *(Comité français d'accréditation)* is responsible for the technical accreditation of candidate conformity assessment bodies.[491] Building upon this accreditation, ANSSI acts as the

[488] Hungary, Act CXXXV of 2025 on the Implementation of the European Union Cyber Resilience Regulation in Hungary and the Amendment of Certain Cybersecurity Provisions. Hungarian Gazette (Magyar Közlöny), No. 158, 29 December 2025, Section 9 (inserting Sections 80/H and 80/I on Market-surveillance into Act LXIX of 2024 on Cybersecurity). Available at: https://magyarkozlony.hu/dokumentumok/adbf9bdb4753d3f6e020f3486f3a3e3ff734cb9e/megtekintes (Accessed 4 July 2026).

[489] Hungary, Act CXXXV of 2025, Section 10 (inserting Articles 80/C through 80/G governing notification, registration, and supervisory reviews).

[490] Hungary, Act CXXXV of 2025, Section 12 (inserting Article 80/I governing administrative enforcement penalties and fine calculations).

[491] France, (2008). *Loi n° 2008-776 du 4 août 2008 de modernisation de l'économie* (LME) [Economic Modernisation Act], which formally designated the Comité français d'accréditation (COFRAC) as France's sole national accreditation body pursuant to Regulation (EC) No 765/2008. *Journal Officiel de la République Française* (JORF), No. 0181. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000019283050 (Accessed 29 September 2026).

notifying authority, formally designating the notified bodies to the European Commission and other member states, while retaining the overarching authority to control and monitor them.[492]

This creates a two-step institutional process in which technical competence is assessed through the national accreditation system, while formal notification remains linked to the national cybersecurity authority. At the same time, CRA vulnerability and incident reports for manufacturers whose main establishment is in France are expected to be routed through CERT-FR, ANSSI's operational CSIRT, via the ENISA single reporting platform.[493] This separates the reporting function from the market-surveillance function, while maintaining a strong role for ANSSI in technical coordination.

Market-surveillance represents another important point of divergence. The French framework purposes assigning CRA market-surveillance responsibilities to *the Agence nationale des fréquences (ANFR)*, with ANSSI providing technical support.[494] This differs from the Hungarian model, where SZTFH concentrates both notification and market-surveillance functions, and from the German model, where CRA implementation is embedded within the broader technical and certification capacities of the BSI. The French approach therefore reflects a distributed model in which cybersecurity expertise, accreditation, notification, incident routing, and market-surveillance are institutionally separated but coordinated.

From a comparative perspective, the operationalization of the CRA demonstrates that institutional divergence persists across different Member States implementing the same EU regulation. Germany would unify technical evaluation and market-surveillance within BSI as a single authority; Hungary concentrates regulatory oversight and enforcement within the SZTFH;

[492] France, Cyber Resilience Act (CRA) – Cybersecurity of Products with Digital Elements, ANSSI guidance, https://cyber.gouv.fr/reglementation/cybersecurite-des-produits/cyber-resilience-act/ (Accessed 4 July 2026).
[493] European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), Article 14. See also Agence nationale de la sécurité des systèmes d'information (ANSSI), *Cadre réglementaire du CRA : Gestion des vulnérabilités et notification*, designating CERT-FR as the national CSIRT coordinator for routing reports submitted via the ENISA Single Reporting Platform (SRP). Available at: https://cyber.gouv.fr/reglementation/cybersecurite-des-produits/cyber-resilience-act/cadre-r%C3%A8glementaire-du-cra/ (Accessed 29 September 2026).
[494] France, Draft Law on Various Provisions for Adaptation to European Union Law (DDADUE Bill), Senate Text No. 347 (2025–2026), 2026, Article 32. Available at: https://www.senat.fr/rap/l25-347/l25-347_mono.html (Accessed 4 July 2026).

and France distributes accreditation, notification, reporting, and surveillance across COFRAC, ANSSI, CERT-FR, and ANFR.

This comparative variation demonstrates that EU implementation diversity is not merely a consequence of administrative weakness; it also reflects different legitimate institutional designs. Consequently, the regulatory efficacy of the CRA depends not solely on uniform statutory mandates, but on the administrative capacity of national authorities to support manufacturers, manage conformity assessments, and execute continuous market-surveillance.

The experiences of Germany, France, and Hungary provide important lessons for Jordan regarding the gradual development of cybersecurity assurance and conformity assessment mechanisms. The comparison demonstrates that effective cybersecurity assurance depends not simply on adopting conformity assessment or certification requirements, but on establishing the institutional capacity necessary to support accreditation, technical evaluation, market-surveillance, regulatory oversight, and compliance enforcement.

At the same time, the three Member States illustrate that these objectives may be achieved through different institutional models reflecting national administrative capacities and regulatory traditions. Accordingly, the principal lesson for Jordan is not the direct transplantation of the full CRA framework may impose institutional and economic demands that would require substantial preparatory capacity-building in Jordan, but the gradual development of a national cybersecurity assurance framework built upon existing regulatory structures. Such an approach would enable Jordan to strengthen the institutional foundations of cybersecurity assurance in a manner that remains proportionate to its regulatory capacities and market conditions while drawing upon selected principles of EU cybersecurity governance.

VI.3 Challenges and Opportunities for the Adaptation of EU Cybersecurity Governance Principles in Jordan

VI.3.1 Institutional and Administrative Capacity Challenges

One of the most significant challenges associated with the adaptation of EU cybersecurity governance principles in Jordan relates to institutional and administrative capacity.[495] As demonstrated throughout the preceding sections, the practical implementation of EU cybersecurity

[495] AL-MUHAISEN et al., 2024, p.858.

legislation depends not only upon the existence of legal obligations but also upon a highly developed institutional ecosystem comprising specialized supervisory authorities, certification bodies, conformity assessment structures, incident-response networks, and regional coordination mechanisms.[496] The implementation experiences of Germany, France, and Hungary further illustrate that even within the EU, the effectiveness of cybersecurity governance is closely linked to institutional capacity, technical expertise, and administrative resources.

By contrast, cybersecurity governance in Jordan remains concentrated primarily within the NCSC, which performs strategic, regulatory, supervisory, operational, and coordination functions.[497] While this centralized structure may facilitate decision-making and policy coherence, it simultaneously places extensive responsibilities upon a relatively limited institutional framework.

Unlike the European model, where cybersecurity responsibilities are distributed across multiple specialized institutions operating at both national and supranational levels, Jordan does not yet appear to have an equivalent institutional structure specifically dedicated to CRA-style product cybersecurity conformity assessment, notified-body supervision, and EU-type market surveillance. Consequently, the adaptation of increasingly sophisticated cybersecurity governance models may encounter significant institutional constraints irrespective of the quality of the underlying legal framework.

Institutional capacity is also closely linked to the availability of financial and technical resources. The implementation of advanced cybersecurity governance mechanisms, particularly those involving conformity assessment, certification, product-security supervision, and large-scale incident coordination, requires sustained public investment in specialized personnel, technical infrastructure, and regulatory oversight.

However, recent budgetary allocations to the NCSC indicate that, while funding continues to support operational activities and core cybersecurity initiatives, the general budget does not identify a dedicated allocation for the development of dedicated certification or conformity assessment mechanisms for digital products. This suggests that Jordan's current resource allocation

[496] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Articles (8,9,10,11,12) and (15,16).
[497] Jordan, Cybersecurity Law No. 16 of 2019, Article 6(B).

remains focused primarily on strengthening core cybersecurity functions rather than expanding the institutional infrastructure required for more sophisticated regulatory models such as those introduced by the CRA.[498]

These financial constraints contrast with the extensive support available to EU Member States through mechanisms such as the Digital Europe Program, Horizon Europe, the Recovery and Resilience Facility, and the expanding operational budget of ENISA. To this extent, the European Commission has allocated approximately €1.3 billion under the Digital Europe Program for the period 2025–2027, covering strategic areas including cybersecurity, AI, cloud and data, and digital skills.[499] The disparity between the EU and Jordan's framework highlights the practical difficulties that may arise when attempting to replicate highly resource-intensive governance models within a more constrained institutional environment.

Beyond financial considerations, the development of effective cybersecurity governance depends upon the availability of specialized technical expertise and administrative capacity. Recent national assessments have identified workforce shortages, limited advanced threat-detection capabilities, uneven incident-response preparedness, and constraints in specialized cybersecurity skills as continuing challenges. These issues are particularly significant in areas such as conformity assessment, vulnerability management, market-surveillance, cyber-threat intelligence, and regulatory enforcement, all of which require highly specialized personnel and sustained technical training.[500]

Furthermore, effective cybersecurity governance increasingly depends upon regional information-sharing mechanisms and cross-border cooperation comparable to those developed

[498] General Budget Law for the Financial Year 2026, Chapter 3210 (National Cybersecurity Center), p.7163. The 2026 General Budget allocates approximately JOD 12.5 million to the National Cybersecurity Center, compared with approximately JOD 18 million in 2025. While the 2026 budget includes JOD 615,000 for technical infrastructure development and increased allocations for salaries, services, and selected cyber intelligence projects, it also reflects a reduction of approximately JOD 2.894 million in funding for cybersecurity incident response and handling. available at: https://www.gbd.gov.jo/uploads/files/gbd/law-min/2026/ar/3210.pdf?v=aa01f537-0f16-4b23-8893-896d75d679f8 (Accessed 7 April 2026).

[499] European Commission, Work Program 2025–2027 of the Digital Europe Programme (DIGITAL). European Commission, 28 March 2025. Available at: https://digital-strategy.ec.europa.eu/en/library/work-programme-2025-2027-digital-europe-programme-digital. (Accessed 9 July 2026).

[500] ALMOMANI et al., 2026, p.30.

within the EU through ENISA, the CSIRTs Network, EU-CyCLONe, and the Cyber Solidarity framework.

While Jordan has made significant progress through the National Cybersecurity Strategy 2025–2028 and the expanding role of the NCSC,[501] the absence of comparable regional institutional mechanisms within the Arab region continues to constrain opportunities for collective capacity building, operational coordination, and cross-border cyber resilience. These limitations demonstrate that the successful adaptation of EU cybersecurity governance principles requires not only legislative reform but also sustained investment in institutional development, technical expertise, and regional cooperation.

VI.3.2 Regulatory Complexity and Compliance Burdens

A second challenge concerns the increasing regulatory complexity associated with contemporary EU cybersecurity legislation. As demonstrated throughout this chapter, instruments such as the NIS2 Directive and the CRA establish comprehensive obligations extending beyond general cybersecurity requirements to encompass risk management, incident reporting, vulnerability management, conformity assessment, technical documentation, continuous monitoring, and regulatory oversight.[502] Although these measures strengthen cybersecurity governance, they also impose significant compliance obligations on both regulated entities and supervisory authorities.[503]

The experience of EU Member States demonstrates that regulatory complexity remains a practical challenge even within comparatively mature institutional environments. Despite the harmonizing objectives of the NIS2 Directive, differences in supervisory arrangements, compliance procedures, and enforcement practices continue to generate variations in how cybersecurity obligations are interpreted and applied.[504]

---

[501] Jordan, National Cybersecurity Center, National Cybersecurity Strategy 2025–2028. Available at: https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/national_cybersecurity_strategy_2025-2028.pdf (Accessed 9 July 2026).

[502] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Articles (20, 21, 23, 31,32,33). See also European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), Articles (6,14,15,27,52).

[503] European Cyber Security Organization, NIS2 Implementation: Challenges and Priorities. White Paper, January 2025. Available at: https://ecs-org.eu/ecso-uploads/2025/01/ECSO-NIS2-White-Paper.pdf (Accessed 15 June 2026).

[504] SAŁEK – FAJDEK, 2025, p.47.

Similarly, the CRA introduces extensive lifecycle obligations requiring manufacturers to manage conformity assessment, vulnerability disclosure, product security, technical documentation, and post-market compliance throughout the lifecycle of products with digital elements.[505] These experiences demonstrate that legal harmonization alone does not eliminate compliance complexity, particularly where supervisory practices and institutional arrangements continue to differ across jurisdictions.

These challenges are likely to be amplified within the Jordanian context due to differences in institutional capacity and organizational maturity. Although Jordan has made significant progress in developing its national cybersecurity framework, the adaptation of sophisticated regulatory models such as the NIS2 Directive and the CRA would require many organizations to comply with obligations that may exceed their current operational capacities. This challenge is particularly relevant for SMEs, which constitute approximately 98 per cent of enterprises in Jordan and frequently operate with limited cybersecurity resources, governance structures, and specialized expertise.[506]

Accordingly, the principal challenge extends beyond the formal adoption of cybersecurity obligations and concerns the regulatory absorptive capacity of regulated entities. Effective compliance requires organizations to possess sufficient institutional maturity, technical expertise, governance capabilities, and operational processes to translate legal obligations into everyday practice.

Evidence from studies examining SME implementation of the NIS2 Directive indicates that compliance is frequently constrained by limited cybersecurity expertise, varying levels of organizational maturity, shortages of skilled personnel, and difficulties integrating cybersecurity governance into existing business processes.[507] As a consequence, many SMEs struggle to conduct

[505] CHIARA, 2025, p.472. See Also European Parliament and Council of the European Union, Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), Articles (6,11,14,15,22,23,24,30).
[506] United States, U.S. International Trade Administration, Jordan Country Commercial Guide – Information and Communication Technology. 26 February 2026. Available at: https://www.trade.gov/country-commercial-guides/jordan-information-and-communication-technology (Accessed 11 July 2026).
[507] JOSWIG – KURZ, 2025, p.17.

risk assessments, interpret regulatory requirements, implement security controls, manage incident reporting, and sustain ongoing compliance without external technical or legal support.[508]

These challenges are further compounded by the increasing technological sophistication of modern cybersecurity regulation. In practice, effective implementation of cybersecurity obligations may require organizations to deploy or maintain technical capabilities such as security monitoring, vulnerability-management processes, incident-detection systems, and appropriate security infrastructure.[509]

While these technologies substantially enhance cybersecurity resilience, they also require specialized expertise and organizational capacity to deploy, maintain, and continuously update them. Organizations operating legacy systems or relying upon outdated digital infrastructure may therefore encounter significant obstacles in achieving effective compliance.

Regulatory complexity also generates legal uncertainty. European experience demonstrates that organizations frequently encounter difficulties interpreting cybersecurity obligations, understanding reporting requirements, identifying competent authorities, and navigating overlapping regulatory frameworks.[510] Such uncertainty may encourage formalistic compliance focused primarily on satisfying procedural requirements rather than achieving substantive improvements in cybersecurity resilience. Similar challenges are likely to arise in Jordan, where cybersecurity regulatory expertise remains concentrated within a relatively limited number of institutions and professionals.

Consequently, the principal regulatory challenge for Jordan is not only the cost of compliance but ensuring that regulatory obligations remain proportionate to the institutional capacities of regulated entities.[511] Rather than replicating the comprehensive obligations established under the NIS2 Directive and the CRA, future regulatory reforms should adopt proportionate and scalable compliance models reflecting organizational size, sectoral risk, and institutional capability.

---

[508] ALI et al., 2025, p.17.
[509] ARROYABE et al., 2024, p.9.
[510] European Cyber Security Organisation (ECSO): NIS2 Implementation: Challenges and Priorities. White Paper, January 2025. Available at: https://ecs-org.eu/ecso-uploads/2025/01/ECSO-NIS2-White-Paper.pdf (Accessed 10 June 2026).
[511] ALMOMANI et al., 2026, p.30.

This could include simplified guidance for SMEs, sector-specific implementation roadmaps, cybersecurity advisory services, workforce development initiatives, public-private partnerships, and targeted support mechanisms that enable organizations to strengthen cybersecurity governance progressively while avoiding disproportionate administrative and economic burdens.[512]

VI.3.3 National and Regional Cooperation Challenges

VI.3.3.1 National Collaboration Challenges

In addition to institutional capacity and regulatory complexity, the effectiveness of cybersecurity governance depends upon the ability of national actors to coordinate their activities within a coherent governance framework. Contemporary cybersecurity threats frequently cut across institutional, sectoral, and organizational boundaries, requiring close cooperation between regulators, incident response authorities, law-enforcement agencies, critical infrastructure operators, private-sector entities, and civil society actors. Consequently, cybersecurity governance is increasingly viewed not merely as a regulatory function but as a coordination challenge requiring continuous information sharing, joint decision-making, and operational cooperation.[513]

Although Jordan has established the NCSC as the central coordinating authority for cybersecurity governance, concentrating strategic, regulatory, supervisory, operational, and coordination responsibilities within a relatively limited institutional framework may create governance challenges as the cybersecurity ecosystem becomes increasingly complex.

The NCSC is responsible for coordinating cybersecurity activities, facilitating information exchange, and cooperating with national institutions,[514] while the National Cybersecurity Council provides strategic oversight through the approval of cybersecurity strategies, policies, and coordination initiatives.[515] Unlike the more functionally differentiated governance arrangements observed within the EU, Jordan's centralized institutional model may encounter increasing pressure as regulatory responsibilities continue to expand.

[512] AL-KAYED et al., 2024, p.15.
[513] AL-KASASSBEH et al., 2023, p.355.
[514] Jordan, Cybersecurity Law No. 16 of 2019, Article 6(B/7).
[515] Ibid., Article 4(B).

One important challenge concerns coordination between cybersecurity authorities and law-enforcement institutions. Effective responses to cyber incidents frequently require close cooperation between technical incident-response bodies and criminal investigation authorities, particularly when cyber incidents involve both operational disruption and potential criminal conduct.

Hungary illustrates this integrated approach through cooperation between the National Cybersecurity Center and specialized law-enforcement authorities. Under Hungary's cybersecurity framework, competent authorities and incident-response bodies are required to cooperate and exchange relevant information when cybersecurity incidents may involve criminal activity.[516] This cooperation aims to ensure that technical mitigation measures are complemented by criminal investigations where necessary.

By contrast, Jordan's NCSC and the Cybercrime Unit, which is the specialized law-enforcement authority responsible for investigating cybercrimes, operate under separate institutional mandates. This separation between technical cybersecurity functions and criminal enforcement responsibilities may create coordination challenges, particularly where the Cybersecurity Law does not appear to establish a detailed statutory cooperation mechanism between these institutions comparable to the specific mechanisms identified in the European examples. Such gaps may affect timely information sharing, preservation of digital evidence, incident attribution, and the coordination of operational responses.

A secondary governance impediment lies in the institutionalization of public-private cooperation.[517] Given the significant role of private-sector entities in operating and securing critical information infrastructure, effective cooperation between public authorities and private operators is an important component of national cyber resilience.[518] However, where primary legislation lacks statutory non-punitive safe harbors and codified disclosure protections, the

[516] Hungary, Act LXIX of 2024 on the Cybersecurity of Hungary, Section 76(1)–(2), National Legislation Database (Nemzeti Jogszabálytár); National Cyber Security Centre of Hungary, "Incident Management – Co-operation, Interaction and Disclosure of Information", stating that NCSC Hungary provides full cooperation to law-enforcement officers, including information required for investigations, in accordance with law. Available at https://njt.jog.gov.hu/jogszabaly/en/2024-69-00-00 (Accessed 30 September 2026).
[517] AL-MUHAISEN et al., 2024, p.858.
[518] Jordan, National Cybersecurity Center, National Cybersecurity Strategy 2025–2028, 2025, available at: https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/national_cybersecurity_strategy_2025-2028.pdf (Accessed 19 January 2026).

regulatory framework may create disincentives for reporting and vulnerability disclosure.[519] Consequently, the absence of robust public-private partnership mechanisms may reduce the timely exchange of threat intelligence and limit the effectiveness of national incident response efforts.

Cybersecurity awareness represents a further coordination challenge. Effective governance depends not only upon capable institutions but also upon a broader cybersecurity culture extending across public institutions, private organizations, and individual users.[520] Although Jordan has made significant progress through the National Cybersecurity Strategy and awareness initiatives led by the NCSC,[521] differences in cybersecurity awareness, technical expertise, and organizational preparedness continue to influence the overall level of national cyber resilience.[522]

From a governance perspective, these comparative observations demonstrate that national cyber resilience depends not only upon the formal existence of statutory mandates, but upon the institutional alignment between technical regulatory authorities, criminal justice bodies, and private infrastructure operators. In Jordan, the institutional division between the technical mandate of the NCSC and the criminal enforcement jurisdiction of the Cybercrime Unit, combined with the absence of statutory safe-harbor mechanisms for private-sector threat disclosure, creates operational friction that mirrors the coordination challenges observed during early European regulatory initiatives.

VI.3.3.2 Regional Cooperation Challenges

A final challenge concerns the relationship between national cybersecurity governance and regional cooperation mechanisms. The comparative analysis undertaken in this chapter demonstrates that, despite the implementation diversity that exists among EU Member States, the European cybersecurity framework benefits from an extensive system of supranational coordination capable of mitigating many of the practical difficulties associated with regulatory diversity. Consequently, the effectiveness of EU cybersecurity governance does not depend exclusively upon national implementation measures but also upon institutional regional structures

[519] CASTALDO – SERINI, 2024, p.189.
[520] NAGYFEJEO – VON SOLMS, 2020, p.20.
[521] Jordan, National Cybersecurity Center, National Cybersecurity Strategy 2025–2028, 2025, available at: https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/national_cybersecurity_strategy_2025-2028.pdf (Accessed 19 January 2026).
[522] ALSOBEH et al., 2023, p.15.

that facilitate cooperation, information sharing, operational coordination, and collective cyber resilience across Member States.

This cooperative architecture is reflected in the complementary roles performed by ENISA, the CSIRTs Network, EU-CyCLONe, and the European Cybercrime Center (EC3).[523] Collectively, these institutions and networks support technical guidance, incident response, strategic crisis management, cybercrime investigations, threat intelligence, and policy coordination, thereby reducing the practical consequences of implementation fragmentation through permanent mechanisms for cooperation and information exchange.[524]

By contrast, Jordan's cybersecurity governance framework remains primarily national in orientation. Although the NCSC serves as the principal institutional actor responsible for coordinating cybersecurity activities and facilitating cooperation with regional and international partners,[525] Jordan does not operate within a regional cybersecurity architecture comparable to that established within the EU.

While Jordan participates in bilateral and multilateral initiatives and has actively engaged in Arab regional cybersecurity and cybercrime cooperation frameworks, such cooperation remains considerably less institutionalized, less operationalized, and less integrated than the EU model.[526] In particular, the absence of a supranational cybersecurity framework comparable to the EU's mechanisms limits the extent to which regional actors can achieve coordinated prevention, incident response, information sharing, and enforcement efforts.

The challenges associated with regional cooperation are not merely institutional but also structural and operational. The EU benefits from a relatively advanced framework of legal harmonization, common regulatory objectives, integrated digital markets, and established

---

[523] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Articles (15,16). See also Europol, "European Cybercrime Centre – EC3: Combating crime in a digital age", European Union Agency for Law Enforcement Cooperation (Europol). Available at https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/european-cybercrime-centre-structure-and-collaboration (Accessed 30 September 2026).

[524] European Union Agency for Cybersecurity, Four EU Cybersecurity Organisations Enhance Cooperation. 23 May 2018. Available at: https://www.enisa.europa.eu/news/enisa-news/four-eu-cybersecurity-organisations-enhance-cooperation (Accessed 12 July 2026).

[525] Jordan, Cybersecurity Law No. 16 of 2019, Article 6(b/5).

[526] Jordan, National Cybersecurity Center: International Cooperation. Available at: https://ncsc.jo/Ar/List/intl_cooperation (Accessed 15 July 2026).

supranational institutions capable of facilitating collective action. By contrast, the Arab region continues to exhibit significant differences in cybersecurity legislation, institutional capacity, digital maturity, political priorities, and regulatory approaches.[527]

Although regional instruments such as the Arab Convention on Combating Information Technology Crime provide a legal basis for cooperation, their operational mechanisms remain considerably more limited than the mechanisms available within the EU.[528] Whereas European cooperation is supported by permanent operational networks, technical coordination platforms, and common regulatory frameworks, regional cooperation in the Arab context remains largely dependent upon intergovernmental coordination and traditional legal-assistance procedures.

These limitations are particularly evident in relation to operational cooperation. Effective cybersecurity governance increasingly requires the rapid exchange of technical information, threat intelligence, incident notifications, and digital evidence across borders. Within the EU, these objectives are supported through permanent operational coordination mechanisms such as the CSIRTs Network and EU-CyCLONe.

By comparison, regional cybercrime cooperation available to Jordan continues to rely primarily upon mutual legal assistance procedures, which may prove insufficiently responsive during rapidly evolving cyber incidents. The Budapest Convention addresses this limitation through its 24/7 Network of Contact Points, facilitating immediate communication between competent authorities for the preservation of electronic evidence and the coordination of investigations. [529] While institutional frameworks exist under Arab Convention on Combating Information Technology Offences, these mechanisms do not provide a directly comparable, treaty-based 24/7 operational network for real-time cyber-incident coordination, expedited preservation of electronic evidence, and related cross-border assistance.

[527] ABU-TAIEH et al., 2018, p.48.
[528] League of Arab States: Arab Convention on Combating Information Technology Offences, Cairo, 21 December 2010. Available at: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf (Accessed 15 July 2026).
[529] Council of Europe, Convention on Cybercrime (Budapest Convention), European Treaty Series No. 185. Budapest, 23 November 2001, Article 35 Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 (Accessed: 15 July 2026).

Similar challenges arise in relation to cross-border access to electronic evidence. Contemporary cyber incidents frequently involve cloud services, foreign service providers, and digital infrastructure distributed across multiple jurisdictions.[530] While the Arab Convention on Combating Information Technology Crime requires States Parties to establish procedures for the preservation and disclosure of electronic data by entities within their jurisdiction, it does not provide mechanisms for direct cross-border access to electronic evidence or streamlined cooperation with foreign service providers.[531]

By contrast, the Second Additional Protocol to the Budapest Convention introduces more advanced procedures for obtaining subscriber information and electronic evidence across jurisdictions, thereby reducing reliance on traditional mutual legal assistance processes.[532] Although these mechanisms enhance the efficiency of cross-border investigations, they have also generated concerns regarding national sovereignty, judicial oversight, and data protection. For Jordan, this illustrates the need to strengthen regional mechanisms for digital-evidence cooperation while ensuring that any future reforms remain compatible with domestic legal safeguards.

Jurisdictional coordination presents an additional challenge where multiple states claim jurisdiction over the same cyber incident. Although both the Arab Convention on Combating Information Technology Crime and the Budapest Convention establish jurisdiction primarily on the basis of territoriality and nationality, the Arab Convention additionally permits jurisdiction where a cybercrime affects a state's vital interests, a concept that remains broadly defined.[533]

By contrast, Article 27(5) of the Budapest Convention specifically encourages consultations between States Parties to determine the most appropriate forum for prosecution in

[530] HOSSAIN, 2023, p.143.
[531] League of Arab States, Arab Convention on Combating Information Technology Offences, Cairo, 21 December 2010. Article 30, Available at: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf (Accessed 15 July 2026).
[532] Council of Europe, Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No. 224), Strasbourg, 12 May 2022. Articles (6,7,8,9,10,11,12) Available at: https://www.coe.int/en/web/cybercrime/second-additional-protocol (Accessed 14 April 2026).
[533] League of Arab States, Arab Convention on Combating Information Technology Offences, Cairo, 21 December 2010. Article 4, Available at: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf (Accessed 15 July 2026).

cases of concurrent jurisdiction, providing a more structured mechanism for managing jurisdictional conflicts.[534]

From a comparative-law perspective, evaluating regional cybersecurity governance across the EU and the Arab region requires clear methodological delimitation. The EU operates as an integrated supranational legal order anchored in harmonized statutory mandates, judicial enforceability, and permanent institutional mechanisms such as ENISA, the CSIRTs Network, and EU-CyCLONe.

In contrast, regional cooperation within the Arab framework is organized along strictly intergovernmental lines, reliant on voluntary collaboration, sovereign consensus, and traditional mutual legal assistance treaties without supranational oversight.[535] Consequently, the EU framework serves in this analysis not as an institutional template for uncritical regional transplantation, but as a functional comparator illustrating the structural prerequisites, information-sharing channels, and operational coordination mechanisms necessary to manage cross-border cyber threats across sovereign jurisdictions.

These differences demonstrate that effective cybersecurity governance increasingly depends upon the interaction between national regulatory capacity and regional institutional cooperation. Cyber threats transcend national borders, while functions such as incident response, cyber-threat intelligence, vulnerability disclosure, cybercrime investigations, supply-chain security, and crisis management increasingly require coordinated action extending beyond individual jurisdictions.

For Jordan, the comparative assessment indicates that a principal limitation of the regional governance environment is the absence of sufficiently operationalized multilateral coordination mechanisms comparable to those developed within the EU. This does not imply that supranational institutional arrangements are either necessary or directly transferable to the Arab regional context. Rather, given the different political, legal, and institutional foundations of regional integration, the European experience demonstrates the value of establishing structured and operational

[534] Council of Europe, Convention on Cybercrime (Budapest Convention), European Treaty Series No. 185. Budapest, 23 November 2001. Article 27(5). Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 (Accessed 15 July 2026).
[535] PAULOVICS – ALBUSTANJI, 2026, p.38.

mechanisms for cross-border cooperation, particularly in information sharing, technical coordination, incident response, and cybercrime cooperation.

VI.4 Summary of Comparative Findings Among Selected EU Member states

The operational assessment across Germany, France, and Hungary demonstrates that the three Member States illustrate different institutional approaches to implementing EU cybersecurity requirements: a highly codified federal regulatory and supervisory framework in Germany, strong centralized operational coordination centered on ANSSI in France, and strong supervisory control supported by mandatory cybersecurity audits in Hungary. This divergence confirms that statutory harmonization does not produce uniform operational execution; rather, regulatory outcomes remain inherently dependent upon the institutional architecture and administrative capacity of each implementing state.

From a regulatory design perspective, two overarching lessons emerge from the European trajectory. First, in dynamic areas such as risk management and incident disclosure, effective governance requires an institutional equilibrium between primary statutory benchmarks and adaptive technical guidance. Second, horizontal product-security and conformity assessment regimes (such as the CRA) are institutionally and administratively demanding, requiring appropriate technical expertise, conformity assessment capacity, accreditation infrastructure, and sustained market-surveillance capabilities.

For Jordan, these findings illustrate the structural risks of normative legal transplantation. When a legal system characterized by centralized administrative authority and resource-constrained market actors attempts to adopt regulatory frameworks designed for advanced, distributed single markets, a structural mismatch occurs between statutory ambition and practical absorptive capacity. Moreover, the limited availability of operational regional cybersecurity networks within the Arab context leaves Jordan comparatively dependent on bilateral and traditional inter-state mechanisms, underscoring that cross-border cyber resilience cannot be achieved through domestic legislative development alone.[536]

Ultimately, the European implementation experience demonstrates that modern cybersecurity regulations cannot be evaluated solely by its doctrinal sophistication, but by its operational

[536] ALRAMAMNEH – ABUANZEH, 2023, p.346.

sustainability within a given economic and institutional context. Having established this diagnostic baseline, Chapter VII articulates a structured, context-sensitive roadmap for strengthening cybersecurity governance against cyber threats in Jordan through a phased program of targeted legislative, institutional, and operational reforms.

Chapter VII: Roadmap for Cybersecurity Governance Reform in Jordan

VII.1 Purpose and Scope of the Roadmap

The preceding chapters established that Jordan possesses an important statutory and institutional foundation for cybersecurity governance, but that this framework remains insufficiently integrated across the cybersecurity lifecycle. The comparative analysis in Chapter V identified structural differences between Jordan and the EU in areas including legal bindingness, risk proportionality, institutional specialization, enforcement, private-sector responsibility, lifecycle continuity, resilience, and operational interoperability. Chapter VI further demonstrated that the effectiveness of cybersecurity regulation depends not only upon legislative design but also upon the institutional, administrative, technical, and economic conditions through which legal obligations are implemented.

The purpose of this chapter is therefore to translate these findings into a practical reform roadmap for strengthening cybersecurity governance in Jordan. The roadmap does not seek to reproduce the EU regulatory model. Instead, it identifies selected legal and institutional principles demonstrated by the comparative and implementation analyses and considers how they may be adapted progressively to Jordan’s administrative, institutional, and economic circumstances.

The proposed reforms are consequently based on the principle of selective and conditional adaptation. European mechanisms are treated as comparative sources from which regulatory principles and implementation lessons may be derived. The objective is to strengthen Jordan's capacity to prevent, manage, respond to, and recover from cyber risks while maintaining proportionality, legal certainty, institutional accountability, and implementation feasibility.

The proposed roadmap is organized around four interconnected areas of reform: legislative reform, institutional governance reform, policy and regulatory reform, and operational and capacity reform. These areas reflect the principal deficiencies identified by the comparative and

implementation analysis and provide the substantive basis for the reforms proposed in the following sections. Their implementation, however, should not be simultaneous or uniform.

This four-dimensional structure also provides a means of avoiding an exclusively legislative approach to cybersecurity reform. A statutory amendment without appropriate institutional responsibility may remain ineffective; institutional restructuring without supporting policy and regulatory instruments may produce unclear implementation; and both may fail where technical expertise, infrastructure, funding, and operational capability are insufficient. Effective reform therefore requires these dimensions to develop in a coordinated and proportionate manner.

VII.2 The Legislative Reform Agenda

VII.2.1 Statutory Modernization of Core Definitions and Crisis Thresholds

The statutory definition of cybersecurity under Article 2 of Cybersecurity Law No. 16 of 2019 must be restructured to eliminate operational breach narratives, such as "deception," "misuse," and "failure to follow procedures", which risks conflating the substantive legal concept of cybersecurity with examples of particular compromise mechanisms.[537] The legislature should reframe cybersecurity strictly around its core normative and protective objective: the measures and capabilities required to ensure the confidentiality, integrity, availability, and authenticity of network and information systems, digital assets, and critical infrastructure, alongside the continuous operational ability to withstand, restore, and maintain service continuity. Removing descriptive mechanics provides legislative precision, standardizes legal terminology across regulatory domains, and relocates specific compliance controls to specialized administrative regulations.

Moreover, Article 2 must be amended to decouple the legal concept of a cybersecurity incident from its restrictive, adversarial framing as merely an intentional "act or attack".[538] The definition should be expanded, drawing upon the NIS2 definition of an incident (Article 6(6) of Directive (EU) 2022/2555), which is not limited to deliberate malicious attacks and encompasses any event that compromises or threatens to compromise the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or the services provided via information

[537] Jordan, Cybersecurity Law No. 16 of 2019, Article 2.
[538] Ibid.

systems.[539] In parallel, the legislature must introduce an explicit primary statutory definition of "cyber threat", drawing upon Article 2(8) of the CSA.[540] This distinction can bridge the gap between latent environmental risks and actualized attacks, thereby establishing precise, objective legal triggers for mandatory incident reporting and administrative risk management.

The legislature should further amend Article 9 of Cybersecurity Law No. 16 of 2019 to establish clear, objective statutory criteria governing the designation of incidents that constitute a "threat to the security and integrity of the Kingdom".[541] Under the current framework, this classification transfers responsibility for managing and directing the response to the NCSC, while requiring relevant parties to comply with its instructions, yet operates without defined qualitative and, where practicable, quantitative criteria. The amended text should explicitly articulate the substantive triggers required for this classification, such as cross-sectoral systemic failure, severe or prolonged disruption of critical infrastructure, or severe cross-border impacts, thereby circumscribing unguided administrative discretion, enhancing legal certainty, and ensuring that emergency response powers are activated only on predictable, risk-calibrated grounds.

VII.2.2 Recalibrating Administrative Enforcement, Sanctions and Judicial Oversight

The legislature should bifurcate the enforcement framework under Article 16 by clearly distinguishing administrative compliance measures from punitive sanctions requiring judicial oversight. The NCSC's direct powers should be confined primarily to proportionate administrative and remedial measures aimed at securing compliance, correcting violations, mitigating risks, and restoring cybersecurity.[542] Conversely, substantial punitive financial penalties (fines exceeding purely administrative thresholds up to 100,000 JOD) must be converted into statutory criminal fines enforceable exclusively by the judiciary.

The NCSC's role in punitive enforcement must be restricted to documenting violations and referring matters requiring criminal adjudication to the Public Prosecutor, for them in turn to transfer it to the competent criminal court for trial in accordance with the applicable rules of

[539] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 6(6).
[540] European Parliament and Council of the European Union, Cybersecurity Act No. 2019/881, Article 2(8).
[541] Jordan, Cybersecurity Law No. 16 of 2019, Article 9.
[542] Ibid., Article 16(A)(6).

jurisdiction, thereby strengthening judicial oversight, procedural safeguards and the separation between administrative compliance supervision and criminal adjudication.

Indeed, Article 5(d) of the 2025 Instructions for Determining the Criteria for Violations of the Provisions of the Cybersecurity Law, Their Controls and the Procedures Due Thereto must be repealed.[543] Instead, the primary legislation must provide for a clear judicial framework governing multi-violation enforcement, leaving the choice and assessment of penalties entirely to the judicial authority, drawing inspiration from Article 4(C) of the Economic Crimes Law.[544]

Under this revised mechanism, every distinct statutory breach, such as concurrent failures in risk assessment, technical documentation, and mandatory incident notification, must generate an independent administrative rectification notice or fine. If multiple breaches are subsequently referred to the judiciary, it is impermissible for the administration to arbitrarily merge or select a single penalty; rather, the competent trial judge must review all concurrent violations and independently decide whether to accumulate the penalties or assess them comprehensively upon a reasoned judicial assessment of proportionality, culpability, and mitigating circumstances.

VII.2.3 Legislative Harmonization between Cybersecurity and Data Protection

The concurrent application of Cybersecurity Law No. 16 of 2019 and PDPL No. 24 of 2023 generates structural friction and procedural duplication across Jordan's digital governance framework, particularly regarding incident reporting mechanisms when an event simultaneously implicates network security and personal data protection. To align technical network defense with personal-data protection, the legislature should amend Article 3 of Cybersecurity Law No. 16 of 2019 to allocate a permanent statutory seat on the National Cybersecurity Council to the Director of the Personal Data Protection Unit.[545] This reform would institutionalize the participation of data-protection expertise in national cybersecurity policy and strategic decision-making.

[543] Jordan, Instructions for Determining the Criteria for Violations of the Provisions of the Cybersecurity Law, Their Controls and the Procedures Due Thereto for the Year 2025, Article 5(d).
[544] Jordan, Economic Crimes Law No. 11 of 1993, Article 4(c).
[545] Jordan, Cybersecurity Law No. 16 of 2019, Article 3.

VII.3 The Institutional Governance Agenda

VII.3.1 Restructuring Strategic Oversight and Council Governance

The first institutional priority requires restructuring the National Cybersecurity Council to transition from a security-centric body toward a balanced, multi-stakeholder governance authority. While Article 3 of Cybersecurity Law No. 16 of 2019 successfully integrates key security and economic institutions,[546] its heavy concentration of military, intelligence, and police representation risks subordinating broader civil, commercial, and fundamental rights considerations to national defense priorities.

Drawing upon the EU's multi-level cybersecurity governance architecture and ENISA's role in coordinating expertise and stakeholder engagement,[547] Jordan should expand the statutory membership of the Council. Specifically, statutory seats should be allocated to independent regulatory authorities—most notably the Personal Data Protection Unit—alongside institutionalized representatives from the academic and scientific research community, consumer and digital rights advocates, and organized private-sector IT industry associations. This rebalancing ensures that national cybersecurity strategies, policy approvals, and budgetary allocations reflect a holistic equilibrium between national security imperatives, civilian supervisory accountability, and the economic needs of digital innovation.

VII.3.2 Realignment of Judicial Police Powers in NCSC and Inspection Safeguards

The operational mandate of NCSC officials acting as judicial police officers under Article 13(a) of Cybersecurity Law[548] must be constrained by mandatory procedural safeguards harmonized with Articles 8 and 48 of the Jordanian Criminal Procedures Law.[549] Non-consensual entry, on-site system audits, and digital device seizures must require prior written authorization from the competent Public Prosecutor or judge, predicated on documented reasonable grounds for suspecting a serious violation. Routine regulatory inspections should be governed by clearly defined statutory powers, notice requirements and procedural safeguards, while intrusive

[546] Ibid., Article 3.
[547] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Articles (18,19). See also European Parliament and Council of the European Union, Cybersecurity Act No. 2019/881, Articles (5,6,9). See also European Union Agency for Cybersecurity (ENISA): ENISA Stakeholder Strategy 2026–2028. 2026. Available at https://www.enisa.europa.eu/publications/enisa-stakeholder-strategy-2026-2028 (Accessed 3 October 2026).
[548] Jordan, Cybersecurity Law No. 16 of 2019, Article 13 (a).
[549] Jordan, Criminal Procedures Law and its Amendments No. 9 of 1961, Articles (8,48).

investigative measures involving entry, search or seizure should be subject to enhanced judicial or prosecutorial safeguards, eliminating extra-judicial overreach and safeguarding private life privacy rights.

VII.3.3 Institutional Specialization and Administrative Capacity

Jordan should adopt a gradual specialization model rather than attempting to reproduce the EU's extensive institutional architecture. The NCSC should retain its strategic and regulatory functions while progressively assigning operational responsibilities to specialized units or accredited bodies for incident response, cybersecurity certification, conformity assessment, and market-surveillance. Priority should initially be given to functions directly required by emerging regulatory obligations, particularly incident response, vulnerability management, and product-security assessment where product-security regulation is introduced.

The NCSC can also issue technical compliance guidelines for regulated entities and conformity assessment bodies, drawing on EU-level technical guidance, including Technical Competence Requirements for CRA Notified Bodies,[550] and the NIS2 Technical Implementation Guidance,[551] because clear technical guidance is necessary to translate statutory cybersecurity obligations into consistent and practically implementable requirements. The experience of Germany, France, and Hungary demonstrates that different institutional configurations can effectively implement EU cybersecurity requirements; Jordan should therefore develop a model adapted to its existing administrative structure rather than creating parallel institutions to NCSC.

VII.4 The Policy and Regulatory Governance Agenda

VII.4.1 Establishing a Risk-Based Cybersecurity Management Framework

Jordan should strengthen its cybersecurity framework by establishing legally defined, risk-based cybersecurity obligations for entities facing significant risks. Building on the NCSC's existing role in national standards and supervision, the reform should move from a predominantly policy-driven and self-assessment approach toward measurable and enforceable requirements.[552] NIS2 provides a useful reference for proportionate risk assessment, supply-chain security, vulnerability

[550] European Union Agency for Cybersecurity, Technical Competence Requirements for CRA Notified Bodies. 4 June 2026. Available at: https://www.enisa.europa.eu/publications/technical-competence-requirements-for-cra-notified-bodies (Accessed 2 September 2026).
[551] European Union Agency for Cybersecurity: NIS2 Technical Implementation Guidance, 26 June 2025, https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance (Accessed 2 September 2026).
[552] ALMOMANI et al., 2026, p.30.

management, incident response, access control, encryption, and business continuity, but these requirements should be introduced progressively to reflect Jordan's institutional capacity and avoid replicating the EU model in full.[553]

Germany illustrates a strongly codified risk-management and supervisory framework; France demonstrates the translation of general statutory obligations through centralized and sector-specific technical coordination; and Hungary places particular emphasis on structured supervisory verification, including registration and periodic cybersecurity audits. Jordan should combine these elements through a national risk-management baseline, sector-specific guidance, and progressively strengthened verification, coordinated centrally by the NCSC.

Implementation should follow a proportionate trajectory to ensure that regulatory obligations remain compatible with the financial, technical, and organizational capacities of Jordanian enterprises. To this extent, implementation should concentrate mandatory, detailed risk-management obligations on critical infrastructure and entities whose disruption poses severe systemic risk, such as banks, energy, telecommunications, and national security sectors.[554]

For these entities, the framework should require documented and periodic risk assessments, appropriate risk-treatment measures, supply-chain and third-party risk management, vulnerability management, business continuity planning, incident preparedness, and other proportionate technical and organizational safeguards. By contrast, lower-risk entities, including many SMEs should initially be subject to simplified and scalable compliance requirements rather than the full regulatory burden applicable to critical entities.[555]

The NCSC should support these organizations through sector-specific compliance roadmaps, standardized documentation templates, simplified assessment procedures, and accessible digital self-assessment tools. Such measures would allow smaller organizations to

[553] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 21(2) (a-j).
[554] Jordan, National Cyber Security Center: Critical Infrastructure Cyber Security Controls (CICSC) Guidance. December 2024. Available at: https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/cicsc_controls_guidance-0.pdf (Accessed 3 October 2026).
[555] ALI et al., 2025, p.17. See Also European Union Agency for Cybersecurity (ENISA): SME Cyber Resilience Maturity Assessment Model. 2026. Available at https://www.enisa.europa.eu/publications/sme-cyber-resilience-maturity-assessment-model (Accessed 3 October 2026).

progressively develop cybersecurity risk-management capabilities while reducing the possibility that regulation itself creates disproportionate barriers to participation and innovation.

Once sufficient institutional expertise, regulatory experience, and market capacity have developed, Jordan should introduce graduated independent verification mechanisms. Critical entities should progressively move beyond internally completed checklists toward formal compliance audits conducted by appropriately qualified and, where feasible, accredited external assessors.

At the same time, sector-specific guidance should be extended to important digital services and other entities presenting elevated cybersecurity risks. The verification regime should remain proportionate: higher-risk entities should be subject to more rigorous and periodic independent assessment, while lower-risk organizations should retain simplified verification mechanisms. This would allow Jordan to develop the institutional foundations for accreditation, auditing, and regulatory supervision incrementally rather than establishing an extensive verification infrastructure before the necessary technical and administrative capacity exists.

This gradually developed approach would address the principal weakness identified in the Jordanian framework embodied in the gap between general policy requirements and measurable, enforceable, risk-calibrated obligations, without reproducing the full administrative complexity of the NIS2 regime. It would also recognize that EU Member States themselves have adopted different institutional mechanisms for implementing substantially similar risk-management obligations, reflecting variations in administrative capacity and regulatory traditions.[556]

Accordingly, the objective should not be the identical transplantation of NIS2, but the gradual development of a Jordanian risk-management model combining legal enforceability, proportionality, technical guidance, supply-chain accountability, and progressive compliance verification. Such an approach would allow regulatory obligations to expand alongside institutional and market capacity, ultimately creating the conditions for a more comprehensive national cybersecurity risk-management regime.

[556] See Chapter VI, Sections VI.2.1–VI.2.3.

VII.4.2 Establishing a Phased Cybersecurity Certification Framework

Jordan should initially establish a voluntary and risk-based cybersecurity certification framework for ICT products, services, and processes, drawing selectively on the EU CSA rather than directly transplanting the mandatory conformity assessment model established under the CRA. The CSA provides an appropriate starting point because its risk-based assurance levels, provision for voluntary conformity self-assessment in low-risk cases, and reliance on common cybersecurity standards offer Jordan a proportionate mechanism for developing product-level cybersecurity assurance without immediately imposing extensive compliance costs on domestic enterprises.[557] This approach is particularly appropriate given Jordan's current limitations in specialized technical expertise, accreditation infrastructure, conformity assessment capacity, and market-surveillance resources.

EU Member States show that cybersecurity certification requires effective institutional support beyond statutory requirements. Germany demonstrates the value of specialized federal technical and supervisory capacity, Hungary of clear regulatory authority and conformity assessment oversight, and France of functionally differentiated but coordinated specialized institutions. Jordan should therefore draw selectively on these models to its institutional context, initially coordinating certification within its existing cybersecurity architecture while progressively developing specialized technical and assessment capacities.

At the same time, the ongoing implementation of the CRA demonstrates that mandatory regulation does not eliminate the need for substantial institutional preparation, even within comparatively mature regulatory systems. The need for Member States to establish or adapt conformity assessment bodies, accreditation arrangements, technical guidance, reporting mechanisms, and market-surveillance structures illustrates the substantial institutional requirements associated with mandatory product-security regulation.[558]

The diversity of German, Hungarian, and French implementation models further demonstrates that there is no single institutional configuration capable of being universally transplanted. Moreover, the CRA itself presents challenges concerning regulatory complexity, product classification, overlapping obligations, compliance costs, and the practical application of

[557] European Parliament and Council of the European Union, Cybersecurity Act No. 2019/881, Articles (52,53,54).
[558] CHIARA, 2025, p.472.

lifecycle cybersecurity requirements.[559] Jordan should therefore use the EU experience not simply as a model for replication, but as a source of institutional and regulatory lessons concerning both the benefits and limitations of increasingly binding certification regimes.

Accordingly, Jordan should adopt a phased certification pathway. During the initial phase, voluntary certification should be introduced with differentiated assurance levels based on product risk, supported by internationally recognized standards and simplified assessment procedures for lower-risk products. Participation should be encouraged through public procurement preferences, regulatory recognition, and other market incentives, while higher-risk ICT products and applications should progressively receive greater regulatory attention.

The framework could draw on internationally recognized standards, including ISO/IEC 27001 for information security management systems.[560] In parallel, product-specific certification should rely on standards and conformity-assessment schemes appropriate to the relevant product category.[561] Therefore, Jordan should develop the institutional foundations required for certification, including assessor competence, accreditation arrangements, technical guidance, vulnerability-management procedures, and basic market-surveillance capabilities.

Once sufficient institutional capacity and market experience have been established, and experience has been accumulated through the initial voluntary certification phase, selected high-risk product categories might gradually be moved from voluntary certification toward mandatory risk-based conformity assessment. This staged approach would allow Jordan to benefit from the CSA's flexibility and market-oriented character, draw upon the institutional lessons of Germany, Hungary, and France, and avoid prematurely assuming the substantial administrative and economic burdens associated with CRA-style mandatory regulation.

[559] AJMERA, 2026, p.5.
[560] International Organization for Standardization (ISO), ISO/IEC 27001 — Information Security Management, available at: https://www.iso.org/isoiec-27001-information-security.html (Accessed 3 October 2026).
[561] CULOT et al., 2021, p.78.

VII.5 The Operational and Technical Capacity Reform Agenda

VII.5.1 Multi-Stage Incident Notification, Significance Thresholds and Bidirectional Threat Intelligence Sharing

Jordan has already established important foundations for reactive cybersecurity governance through the national incident-reporting platform, the Cybersecurity Incident Classification Instructions of 2023,[562] and the Cybersecurity Incident Response and Reporting Policy 2025.[563] The principal weakness is therefore not the absence of reporting mechanisms, but the normative and procedural disconnect between incident classification, reporting triggers, and enforcement.

The primary legislation does not establish sufficiently precise statutory timelines and thresholds for determining when an incident becomes reportable, while Article 9 of the Cybersecurity Law permits an incident to be designated as threatening the security and integrity of the Kingdom without clearly defined criteria.[564] The relationship between this exceptional national-security designation and the existing incident-classification framework is not expressly articulated in the primary legislation, potentially creating uncertainty as to when ordinary incident classification should give rise to Article 9 escalation.

The NCSC/JO-CERT should transition incident reporting from a one-way compliance obligation into a dynamic, two-way threat-intelligence exchange. Integrating lessons from Hungary's comprehensive incident taxonomy under Act LXIX of 2024—which captures significant incidents, broader cyber threats, and near-misses[565]—the NCSC/JO-CERT should systematically analyze reported telemetry, sanitize sensitive commercial data, and redistribute actionable intelligence. The institutional experiences of Germany, France, and Hungary illustrate the importance of national CSIRT analytical and coordinating capacity in receiving, assessing and, where appropriate, redistributing actionable incident information.[566]

---

[562] Jordan, Instructions for the Classification of Cybersecurity Incidents for the Year 2023, issued pursuant to Clause (3) of Paragraph (b) of Article 6 of the Cybersecurity Law No. 16 of 2019, 2023, available at: https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/cyber_security_incidents_categorization_instructions_2023.pdf, (Accessed on 25 January 2026).

[563] Jordan, the National Cybersecurity Center: Cybersecurity Incident Response and Reporting Policy 2025, available at https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/cs_incident_response_and_reporting_policy_2025-0.pdf, (Accessed 2 Sep. 2026).

[564] Jordan, Cybersecurity Law No. 16 of 2019, Articles (8,9).

[565] Hungary, Act LXIX of 2024 on the Cybersecurity of Hungary. Sections (67,68).

[566] SAŁEK – FAJDEK, 2025, p.43.

Jordan should address this deficit through four directly connected reforms: -

First, the NCSC should convert the existing reporting platform into a legally mandated multi-stage notification system. Drawing on Article 23 of NIS2, the system should require: (i) an early warning within 24 hours of awareness of a significant incident; (ii) a substantive incident notification within 72 hours containing the available technical assessment, indicators of compromise, and initial response measures; and (iii) a final report within one month addressing the root cause, operational impact, remediation measures, and longer-term corrective controls.[567] These stages should be incorporated into binding legislation or implementing regulations rather than remaining solely within administrative policy. The existing four-level classification system should determine which incidents trigger each reporting obligation, thereby connecting classification directly to notification and enforcement.

Second, Article 9 should be operationalized through objective national-security thresholds. The legislation or binding implementing rules should define the circumstances in which an incident constitutes a threat to the security and integrity of the Kingdom, using measurable criteria derived from the existing classification framework. Such criteria should include the scale and duration of disruption, the criticality of affected services, cross-sectoral consequences, population impact, compromise of nationally significant systems, and other indicators of systemic harm.

An Article 9 designation should therefore constitute an exceptional escalation mechanism triggered by predefined systemic-risk criteria, rather than an undefined category operating independently from the four-tier classification system. This would preserve the NCSC's capacity for centralized intervention in genuinely systemic incidents while reducing discretionary uncertainty during the response to critical incidents.

Third, the NCSC/JO-CERT should transform incident reporting into a two-way threat-intelligence mechanism. Reporting entities should not merely transmit information to the NCSC; the NCSC/JO-CERT should systematically analyze reported incidents and return actionable threat intelligence to relevant entities. This should include anonymized indicators of compromise,

[567] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 23(4).

emerging attack patterns, technical mitigation measures, and sector-specific warnings, disseminated through standardized machine-readable mechanisms where technically feasible.

The institutional experiences of Germany, France, and Hungary demonstrate that effective reactive governance depends substantially on the analytical and coordinating capacity of specialized cybersecurity authorities and CSIRTs to receive, assess, coordinate, and, where appropriate, share actionable incident information. Jordan should therefore build upon the NCSC's existing central coordinating role to establish a secure national threat-intelligence exchange rather than creating a fragmented network of parallel reporting channels.

Fourth, moving beyond the policy-level requirements established under Cybersecurity Incident Response and Reporting Policy 2025,[568] the regulatory framework must establish legally enforceable post-incident obligations for significant and high-risk incidents. Regulated entities should be required to submit an assessment of the likely root cause and the measures taken to address it within their final one-month report (drawing on Article 23 NIS2), accompanied by a formal remediation plan detailing patch management, malware eradication, and updated business continuity measures.[569] For designated critical national infrastructure, the NCSC should be vested with the supervisory authority to conduct *ex-post* compliance verification audits to ensure that corrective measures are substantively implemented, preventing incident recurrence and closing the governance loop between active containment and continuous cyber resilience.

Implementation should proceed in two stages. The first stage should consolidate the existing platform, classification system, and 2025 reporting policy into a binding national reporting procedure, establish the reporting deadlines and significance thresholds, and define the relationship between ordinary classification and Article 9 escalation. The second stage should integrate automated incident triage, structured threat-intelligence exchange, mandatory root-cause verification audits where proportionate, independent post-incident verification audits, and institutionalized post-incident learning mechanisms, progressively connecting the reporting system with sectoral regulators, critical infrastructure operators, and relevant cybersecurity service

[568] Jordan, the National Cybersecurity Center: Cybersecurity Incident Response and Reporting Policy 2025, available at https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/cs_incident_response_and_reporting_policy_2025-0.pdf, (Accessed 2 Sep. 2026).
[569] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Article 23(4).

providers. This sequence would allow Jordan to increase legal bindingness and operational interoperability without immediately reproducing the institutional complexity of the EU framework.

VII.5.2 Integrated Cybersecurity and Data-Breach Notification

Jordan should establish an integrated breach-notification mechanism between the NCSC and the Personal Data Protection Unit to eliminate duplication and conflicting reporting requirements where a cyber incident also constitutes a personal-data breach.[570] Where legally compatible, a unified electronic notification mechanism should allow a single submission to satisfy overlapping notification requirements, while automatically routing technical incident information to the NCSC/JoCERT and personal-data breach information to the Personal Data Protection Unit.

This mechanism should be complemented by a permanent Joint Technical Liaison Committee between the NCSC and the Personal Data Protection Unit to align technical baseline controls—including technical and organizational measures for the protection of personal data, as well as appropriate encryption and pseudonymization measures where applicable,[571] — and to issue harmonized sectoral compliance guidelines. This institutional connection would bridge technical network resilience with data-protection requirements and reduce jurisdictional fragmentation between the two regulatory regimes.

VII.5.3 Economic and Resource Reform

Jordan should concentrate public investment initially on critical infrastructure and high-risk digital services rather than attempting economy-wide implementation of resource-intensive EU mechanisms. The changes in NCSC budget allocations and incident-response funding identified in the 2026 budget reinforce the need for prioritization available resources toward core cybersecurity capabilities rather than premature institutional expansion.[572]

---

[570] Jordan, PDPL No. 24 of 2023, Articles (18(b), 20).
[571] Ibid., Article 8(b).
[572] General Budget Law for the Financial Year 2026, Chapter 3210 (National Cybersecurity Center), p.7163. The 2026 General Budget allocates approximately JOD 12.5 million to the National Cybersecurity Center, compared with approximately JOD 18 million in 2025. While the 2026 budget includes JOD 615,000 for technical infrastructure development and increased allocations for salaries, services, and selected cyber intelligence projects, it also reflects a reduction of approximately JOD 2.894 million in funding for cybersecurity incident response and handling. available at: https://www.gbd.gov.jo/uploads/files/gbd/law-min/2026/ar/3210.pdf?v=aa01f537-0f16-4b23-8893-896d75d679f8 (Accessed 7 April 2026).

Jordan should establish a dedicated multi-year cybersecurity capacity fund to finance specialized personnel, technical infrastructure, certification capabilities, and regulatory training, while using public-private partnerships and cost-sharing mechanisms for services benefiting commercial operators, governed by transparent eligibility criteria, clear procurement rules, and strict accountability safeguards to avoid regulatory capture.[573] For SMEs, compliance should be supported through standardized tools, guidance, subsidized security assessments, and capacity-building programs rather than immediately imposing CRA-level product-security assessment and, where applicable, third-party conformity-assessment costs. This would enable regulatory modernization without imposing disproportionate economic burdens on Jordanian enterprises.

VII.5.4 National Coordination Reform

To resolve the structural fragmentation between technical risk mitigation and criminal prosecution, Jordan should enact a legally binding coordination framework governing the operational interface between the NCSC and the Public Security Directorate's Cybercrime Unit. Drawing on EU-level cooperation between cybersecurity institutions and law-enforcement authorities, including cooperation involving ENISA, Europol and the EC3,[574] alongside Hungary's statutory Single Point of Contact integration under Act LXIX of 2024,[575] Jordan should amend Cybersecurity Law No. 16 of 2019 to establish a formal case-referral mechanism, where an incident reported to the NCSC reveals prima facie indicators of criminal conduct under the Electronic Crimes Law, such as unauthorized system penetration.[576]

The amended law should require the NCSC to prepare an official Technical Incident Assessment Report to the Cybercrime Unit and the competent Public Prosecutor. This report must document the attack vectors, exploit vulnerabilities, digital system traces, and initial forensic telemetry, while upholding strict evidentiary chain-of-custody standards. This arrangement preserves the distinct mandates of both bodies: the NCSC focuses on rapid technical containment, threat mitigation, and system recovery, while law enforcement leads the formal criminal investigation and perpetrator attribution without jeopardizing technical remediation.

[573] WAH – ZUREIGAT, 2025, p.1050.
[574] European Cybercrime Centre: Combating crime in a digital age", European Union Agency for Law Enforcement Cooperation. Available at https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/european-cybercrime-centre-structure-and-collaboration (Accessed 30 September 2026).
[575] Hungary, Act LXIX of 2024 on the Cybersecurity of Hungary.
[576] Jordan, Electronic Crimes Law No. 17 of 2023.

VII.5.5 Regional Coordination Reform

To overcome the less institutionalized regional cybersecurity coordination architecture in the Arab region, compared with the EU's institutional ecosystem, including ENISA, the CSIRTs Network, and EU-CyCLONe,[577] Jordan should advocate within the League of Arab State, Jordan should advocate within the League of Arab States for the establishment of a specialized Arab Regional Cybersecurity Coordination Center. Operating under a modernized regional framework, this Center would serve as a permanent technical and operational hub tasked with facilitating cross-border cyber incident coordination, standardizing threat taxonomies, and managing an automated, progressively interoperable threat-intelligence exchange mechanisms.

In parallel, to address the acute delays associated with traditional Mutual Legal Assistance under Combating Information Technology Offences, Jordan should progressively align its domestic procedural rules with the procedural and cooperation standards reflected in the Budapest Convention on Cybercrime,[578] and its Second Additional Protocol (CETS No. 224).[579] This requires establishing a dual-track operational mechanism: first, a statutorily empowered 24/7 point of contact within the Public Prosecution dedicated to criminal investigations and digital evidence preservation, in alignment with international frameworks like the Budapest Convention; and second, an enhanced 24/7 technical point of contact within the NCSC/JoCERT for incident coordination. While the 24/7 criminal network facilitates international communication for evidence preservation, lawful cross-border access to electronic evidence held by foreign cloud service providers must rely upon clear statutory legal bases, including mutual legal assistance procedures and, where applicable, the enhanced cooperation mechanisms of the Second Additional Protocol.

[577] European Parliament and Council of the European Union, Directive No. 2022/2555 on the Security of Network and Information Systems (NIS2 Directive), Articles (9,10,11,12).
[578] Council of Europe, Convention on Cybercrime (ETS No. 185), 2001. Article 35.
[579] Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence CETS No. 224, 2022. Articles (7,8,9,10,13,14), Available at https://rm.coe.int/1680a49dab?utm (Accessed 19 September 2026).

Chapter VIII: Conclusion

VIII.1 Research Findings

The central challenge in contemporary cybersecurity governance lies not simply in the existence or absence of legal rules, but in whether those rules form a coherent and enforceable system capable of governing cyber risk continuously across its lifecycle. Cybersecurity becomes legally meaningful only when responsibility does not begin with the occurrence of an incident and end with its investigation or punishment, but extends through the conditions that precede the incident and the measures that follow it.[580]

The adequacy of a cybersecurity framework must therefore be assessed by the relationship between its legal rules, institutional architecture, and operational capacity, rather than by the volume of legislation it contains.[581] This proposition provides the central thread connecting the conceptual analysis, the EU and Jordanian legal examinations, the comparative assessment, the Member-State implementation analysis, and the resulting assessment of regulatory transferability.

Chapter II established the conceptual foundation for this conclusion by demonstrating that cybersecurity cannot be reduced to the criminal-law treatment of cybercrime. Criminal law remains essential for investigation, attribution, prosecution, and deterrence, but its principal function arises in relation to unlawful conduct, rather than the *ex-ante* management of technical, organizational, supply-chain, and human vulnerabilities.[582]

The study consequently treats cybersecurity as a broader legal-governance problem in which the law must anticipate and allocate responsibility for risks before incidents occur, while also providing mechanisms for response, recovery, and institutional learning when preventive measures fail. This distinction provides the conceptual basis for evaluating the effectiveness of both the EU and Jordanian frameworks.

Chapter III demonstrated that the EU has established a multi-layered, multi-instrument regulatory architecture that addresses systemic digital risk through functionally differentiated legal

[580] TEICHMANN, 2025, p.210.
[581] COTTA – RIGHETTINI, 2026, p.3.
[582] European Union Agency for Cybersecurity, Governance Frameworks for National Cybersecurity Strategies (2023), https://www.enisa.europa.eu/sites/default/files/publications/Building%20Effective%20Governance%20Frameworks%20for%20the%20Implementation%20of%20National%20Cybersecurity%20Strategies.pdf?utm (Accessed 20 September 2026).

regimes. Rather than relying on a monolithic statute, the EU framework couples organizational resilience and incident reporting under the NIS2 Directive with institutional coordination and certification under the CSA, mandatory lifecycle product security under the CRA, and data protection under the GDPR, complemented by sectoral frameworks like DORA and the AI Act.[583] Functionally, this architecture exhibits statutory risk proportionality, institutional specialization, and cross-border operational solidarity, while simultaneously generating significant compliance complexity and administrative burdens for regulated entities.[584]

However, Chapter III also established that the comparatively advanced regulatory architecture of the EU is accompanied by significant operational friction. The coexistence of multiple, parallel regulatory regimes can create substantial compliance complexity, overlapping reporting requirements, and significant financial and administrative burdens for economic operators, particularly SMEs. This reveals an important tension between regulatory sophistication and practical feasibility, particularly where organizations must comply simultaneously with requirements arising from different but intersecting regulatory frameworks.

Chapter IV established that Jordan has instituted a foundational legal and institutional architecture for cybersecurity governance, anchored by Cybersecurity Law No. 16 of 2019 and the centralized NCSC.[585] However, the inquiry demonstrated that the national framework remains structurally centralized and primarily reliant on secondary administrative instruments and executive implementation rather than comprehensive statutory codification across the digital lifecycle.

While complementary regimes exist in data protection and electronic crimes, they function largely as discrete statutory silos that lack substantive procedural integration and synchronized incident-escalation pathways. Furthermore, the analysis revealed potential friction between aspects of the administrative enforcement framework and the principles of administrative legality, procedural due process, and the separation of executive oversight from judicial authority.[586] Consequently, the analysis characterizes Jordan's framework as a developing governance model

[583] Directive (EU) 2022/2555 (NIS2); Regulation (EU) 2019/881 (Cybersecurity Act); Regulation (EU) 2024/2847 (Cyber Resilience Act); Regulation (EU) 2016/679 (GDPR); Regulation (EU) 2022/2554 (DORA); Regulation (EU) 2024/1689 (AI Act).
[584] TEICHMANN, 2026, p.14.
[585] Jordan, Cybersecurity Law No. 16 of 2019.
[586] Ibid., Article 16.

in which reactive mechanisms remain more prominent than comprehensive preventive and lifecycle-oriented obligations.

The comparative analysis therefore indicates that the principal structural difference is not whether cybersecurity is legally recognized, but the extent to which legal responsibility is distributed, risk is differentiated, obligations are binding, institutions are specialized, and resilience is maintained throughout the cybersecurity lifecycle.

The application of the Regulatory Maturity Matrix developed in Chapter V demonstrates that the principal structural divergence between the two systems lies in the relationship between legal bindingness, risk proportionality, institutional capacity, private-sector responsibility, lifecycle continuity, resilience integration, enforcement, and operational interoperability. The comparatively higher level of regulatory maturity identified in the EU framework across these dimensions is consistent with its distributed and increasingly lifecycle-oriented governance architecture.

Jordan's approach, while providing an operational administrative foundation and significant centralized capacity, remains comparatively less developed in the statutory codification of preventive and lifecycle obligations, differentiated risk allocation, institutional specialization, and continuous resilience mechanisms.

At the same time, the comparison does not support the conclusion that greater regulatory complexity automatically produces better governance. The EU experience demonstrates that regulatory maturity can generate overlapping obligations, administrative complexity, conformity costs, and significant compliance pressures, particularly for SMEs.[587] The relevant comparison is therefore not between a simply “better” EU model and a “weaker” Jordanian model, but between different regulatory equilibria whose effectiveness depends upon the relationship between legal sophistication, institutional capacity, operational feasibility, and economic absorption capacity.

The answer to the central research question is therefore qualified rather than binary: Jordan possesses the essential institutional and legal foundation upon which a more comprehensive cybersecurity governance system can be built, but its present framework requires further legal and

[587] ALI et al., 2025, p.17.

institutional development to provide a coherent, enforceable, proportionate, and lifecycle-oriented response to the full spectrum of contemporary cyber risks.

The examination of Germany, France, and Hungary demonstrates that the effectiveness of EU cybersecurity regulation depends substantially upon the domestic institutional and administrative conditions through which common European rules are implemented. Despite operating under the same broader EU regulatory architecture, the three Member States translate and operationalize cybersecurity obligations through different institutional configurations, demonstrating that formal EU-level harmonization does not produce identical regulatory outcomes. The implementation experience shows that effective cybersecurity regulation requires more than legislative transposition: it depends upon specialized supervisory capacity, technical expertise, administrative coordination, compliance-monitoring capability, appropriate assurance and accreditation infrastructure, adequate financial resources, and the ability of public authorities and market actors to absorb continuing regulatory obligations.

Germany illustrates the value of detailed statutory codification and specialized institutional capacity; France demonstrates the flexibility that may be achieved through strong technical expertise and administrative guidance; while Hungary shows the potential, as well as the compliance burden, associated with intensive verification and audit mechanisms.

The Member State experience therefore indicates that regulatory sophistication does not itself ensure effective governance: sustainable implementation requires an appropriate relationship between legal certainty, administrative capacity, technical infrastructure, institutional coordination, and proportionality. The significance of the Member-State analysis for Jordan is therefore methodological as much as substantive: legal effectiveness must be assessed through the conditions that make regulatory rules operational, rather than inferred from the formal sophistication of the legislation itself. These findings provide the analytical basis for the phased and context-sensitive reform roadmap developed in Chapter VII.

VIII.2 Recommendations

On the basis of the comparative findings and the reform roadmap developed in Chapter VII, the study proposes the following context-sensitive recommendations for the progressive development of Jordan’s cybersecurity governance framework:

First, Jordan should adopt a phased and context-sensitive approach to cybersecurity regulatory reform. The implementation mechanisms observed in the selected EU Member States should be considered where they are compatible with Jordan's existing legal structure and can be progressively supported by the necessary institutional and economic capacity. The EU acquis should therefore not be reproduced as a uniform model, but selectively adapted to Jordanian legal, institutional, and economic conditions. This approach constitutes a model of conditional transferability, in which regulatory mechanisms are adopted only where their institutional, legal, and economic preconditions can be satisfied. The reform roadmap developed in Chapter VII provides a framework for such conditional transferability, sequencing reforms according to institutional preparedness, regulatory capacity, and implementation feasibility.

Second, Jordan should strengthen the statutory foundations of cybersecurity governance by establishing clearer, more comprehensive, and lifecycle-oriented legal obligations. The current framework should progressively move beyond broad statutory authority and reactive post-breach regulation towards enforceable *ex-ante* obligations covering risk assessment, risk-proportionate classification, vulnerability management and disclosure, incident preparedness, post-incident remediation, and continuous cybersecurity improvement. These obligations should be sufficiently clear and proportionate to provide legal certainty while allowing differentiated requirements according to the level of cyber risk.

Third, Jordan should establish a clearer distribution of institutional responsibilities and strengthen institutional accountability. The concentration of supervisory, technical, and punitive functions within an executive authority should be reconsidered through an institutional structure that clearly distinguishes regulatory oversight, technical cybersecurity functions, compliance supervision, incident response, and judicial or criminal-investigative functions. Such differentiation would strengthen administrative accountability, reduce institutional overlap, and provide clearer boundaries between executive oversight and judicial competence.

Fourth, Jordan should establish a risk-based and proportionate cybersecurity governance framework that allocates obligations according to the nature and level of cyber risk. Rather than applying uniform requirements across entities and sectors, the regulatory framework should progressively introduce differentiated obligations for critical, high-risk, and lower-risk entities. Higher-risk entities should be subject to more comprehensive risk-management, reporting,

verification, and remediation requirements, while obligations imposed on lower-risk entities should remain proportionate and scalable. This approach would strengthen regulatory effectiveness while reducing unnecessary compliance burdens, particularly for entities with more limited institutional and economic capacity.

Fifth, Jordan should strengthen preventive governance, incident accountability, and procedural safeguards across the cybersecurity lifecycle. Cybersecurity regulation should not be centered primarily on penalties following a security incident. It should establish a continuous governance cycle encompassing prevention, preparedness, detection, notification, response, recovery, remediation, and institutional learning. At the same time, administrative enforcement and sanctions should be accompanied by appropriate procedural safeguards, clear legal standards, and effective oversight mechanisms, ensuring that the exercise of cybersecurity powers remains consistent with administrative legality and due process.

Sixth, implementation of these reforms should be supported by sustained institutional, technical, and economic capacity-building. Legislative reform alone cannot ensure effective cybersecurity governance. Jordan should therefore progressively strengthen specialized institutional expertise, technical capabilities, inter-agency coordination, workforce development, and mechanisms for cooperation with the private sector. Reform should be sequenced according to available resources and institutional preparedness so that newly established legal obligations remain practically enforceable rather than creating formal requirements that exceed implementation capacity.

Taken together, these recommendations supports the central hypothesis of the study in its essential form: strengthening Jordanian cybersecurity governance requires greater statutory clarity, differentiated risk allocation, clearer institutional responsibilities, stronger accountability, and more comprehensive preventive and lifecycle mechanisms, while ensuring that these developments remain calibrated to Jordanian institutional and economic realities.

VIII.3 Limitations of the Study

The findings and comparative assessments of this study must be interpreted in light of several methodological, temporal, and doctrinal limitations. The primary methodological limitation arises from the inherent structural asymmetry between the comparative subjects: the study contrasts Jordan’s unitary legal order with the EU’s supranational and multi-level regulatory architecture.

As the EU is an integrated regional bloc rather than a conventional sovereign state, supranational regulations and directives operate alongside divergent domestic administrative and institutional traditions across Member States. Consequently, the comparative inquiry is functional and governance-oriented rather than a direct comparison of identical legal systems. Furthermore, the analysis of domestic implementation in Germany, France, and Hungary was constrained by linguistic barriers, as critical administrative guidance documents and national legislation are predominantly published in their respective national languages, particularly German, French, and Hungarian.

A second critical limitation concerns the temporal boundaries of contemporary EU cybersecurity legislation. Major recent regulatory instruments, most notably the CRA, the Cyber Solidarity Act, the AI Act, and the domestic transposition of the NIS2 Directive, involve staged application, transitional arrangements, or implementation processes extending through 2026 and, in the case of the CRA, into 2027. Given that this dissertation concludes in October 2026, the real-world operational effectiveness and long-term market compliance implications of these emerging regimes cannot yet be assessed comprehensively. Similarly, the study could not incorporate comprehensive sector-by-sector empirical data on the effects of these emerging compliance obligations on SMEs across the selected Member States.

Finally, the inquiry encountered notable doctrinal constraints within the Jordanian legal landscape. Existing scholarship on digital security in Jordan remains predominantly concentrated within computer science, technical engineering, and information-systems literature. Doctrinal legal analyses examining statutory coherence, administrative legality, judicial oversight, and institutional governance remain scarce. The study was therefore required to construct its baseline legal critique through direct primary-source analysis of fragmented legislative and regulatory instruments, including statutes, ministerial regulations, and secondary instructions, especially as specialized legal scholarship and domestic administrative jurisprudence on cybersecurity governance in Jordan remain limited and still developing.

VIII.4 Directions for Future Research

These limitations also identify several directions for future research. Comparative research could extend the analysis beyond Germany, France, and Hungary to additional EU Member States and to Arab and Middle Eastern jurisdictions, allowing researchers to determine whether the

institutional centralization, regulatory gaps, and implementation constraints identified in Jordan represent jurisdiction-specific characteristics or wider patterns.

Furthermore, while this study primarily adopted a doctrinal and functional comparative methodology, future research could incorporate qualitative and empirical field investigations into the practical reception and adaptation of multi-layered European governance principles within Jordan's domestic legal order. Engaging key stakeholders, including representatives of the NCSC, the judiciary, the Cybercrime Unit, operators of critical infrastructure and other regulated entities, and private-sector IT compliance officers, would provide valuable empirical insights into organizational absorptive capacity, administrative enforcement friction, and the real-world operationalization of secondary instructions.

A further area for future research concerns the interaction of parallel European cybersecurity regimes, particularly the potential overlap between the CRA, NIS2, and GDPR. Future scholarship could examine whether greater procedural coordination and interoperable reporting mechanisms are necessary to mitigate overlapping regulatory obligations, reduce cumulative administrative burdens, and preserve legal certainty for regulated entities.

VIII.5 Concluding Remarks

Ultimately, this study demonstrates that effective cybersecurity governance depends not on legislation alone, but on the coherence between legal obligations, institutional responsibility, technical capacity, and regulatory accountability. The EU experience illustrates the potential of a risk-based and lifecycle-oriented governance architecture, while the Jordanian context shows that such mechanisms must be adapted to domestic institutional and economic capacities. The sustainable path for Jordan therefore lies not in replicating the EU model, but in selective adaptation and progressive regulatory maturation, ensuring that law, institutions, and operational capacity function together as a coherent and continuously evolving system of cyber resilience.

LIST OF REFERENCES

Journal Articles

1- ABU et al. 2018 = ABU, M. S. – SELAMAT, S. R. – ARIFFIN, A. – YUSOF, R.: Cyber Threat Intelligence – Issue and Challenges. Indonesian Journal of Electrical Engineering and Computer Science, Vol. 10, No. 1, 2018, pp. 371–379.

2- ABU-TAIEH et al., 2018 = ABU-TAIEH, Evon – AL HADIDI, Ahmad – ABU-TAIEH, Ehab – AL-ZOUBI, Mohammad – AL-KHMAISEH, Omar: Cyber Security Crime and Punishment: Comparative Study of the Laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia. International Journal of Cyber Warfare and Terrorism, Vol. 8, No. 3, 2018, pp. 46–61. DOI: 10.4018/IJCWT.2018070104.
3- ADALJA – LICHTENBERG, 2018 = ADALJA, A. – LICHTENBERG, E.: Produce Growers' Cost of Complying with the Food Safety Modernization Act. Food Policy, Vol. 74, 2018, pp. 23–38.
4- AJMERA, 2025 = AJMERA, P.: Cybersecurity in the Internet of Things: Trends and Challenges in a Nascent Field. Computer Law & Security Review, Vol. 59, 2025, Article 106204, pp. 1–15. DOI: 10.1016/j.clsr.2025.106204.
5- AJMERA, 2026 = AJMERA, P.: European Product Regulation Gets a Security Update – The EU Cyber-Resilience Act as an Adaptation to a Highly Digitized Product Market. European Journal of Risk Regulation, 2026, pp. 1–20. DOI: 10.1017/err.2026.10150.
6- ALBUSTANJI, 2023 = ALBUSTANJI, Huthaifa: Using AI in Cybersecurity within European Union: Double Edge Sword. Revista Facultății de Drept Oradea, Vol. 1, No. 2, 2023, pp. 147–159.
7- ALHARBI et al., 2021 = ALHARBI, F. – ALSULAMI, M. – AL-SOLAMI, A. – AL-OTAIBI, Y. – AL-OSIMI, M. – AL-QANOR, F. – AL-OTAIBI, K.: The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia. Sensors, Vol. 21, No. 20, 2021, Article 6901, pp. 1–14. https://doi.org/10.3390/s21206901.
8- AL-HUSSEINI – JASSIM, 2018 = AL-HUSSEINI, Ammar – JASSIM, Abdul Razzaq: The Integration of Procedural Criminal Rules. Journal of Legal and Political Sciences, Vol. 7, No. 1, 2018, pp. 1–34.
9- ALI et al., 2025 = ALI, Adnan Bin Amanat – AYYASAMY, Ramesh Kumar – AKBAR, Rehan – JEBNA, Abdulkarim Kanaan – ADNAN, Kiran: Cybersecurity Infrastructure Compliance Key Factors to Detect and Mitigate Malware Attacks in SMEs: A Systematic Literature Review. SAGE Open, Vol. 15, No. 1, 2025, pp. 1–19.
10- AL-KASASSBEH et al., 2023 = AL-KASASSBEH, Fahad Yousef – ABU GHAZLEH, Ali Mohammad – KAREEM, Ma'moon Juma'h M. – BREIZAT, Manal Omar: International

and National Efforts to Protect Cyber Security: Jordan Case Study. International Journal of Cyber Criminology, Vol. 17, No. 2, 2023, pp. 350–363. DOI: 10.5281/zenodo.4766720.

11- AL-KAYED et al., 2024 = AL-KAYED, Wael Jamal – ALGHIZZAWI, Mahmoud – ALKLOUB, Rami Sameer Ahmad: The Impact of Cybersecurity on SMEs Strategies Through Technological Infrastructure in Balqa Governorate. Journal of Infrastructure, Policy and Development, Vol. 8, No. 15, 2024, Article 8194, pp. 1–17. DOI: 10.24294/jipd8194.

12- ALMOMANI et al., 2026 = ALMOMANI, Iman – MEHDAWI, Shahed – ALLABADI, Yazeed: Towards Effective Cybersecurity Governance: Jordan Compliance System and Self-Assessment Tools. Journal of Cybersecurity and Privacy, Vol. 6, No. 2, 2026, Article 60, pp. 1–34.

13- AL-MUHAISEN et al., 2024 = AL-MUHAISEN, Heba – ALDABBAS, Ali – ALQAISI, Abeer – ALMOMANI, Sayel – ABU ALZEIT, Rehan: Cybersecurity Challenges in the Hashemite Kingdom of Jordan. South Eastern European Journal of Public Health, 2024, pp. 852–860.

14- ALRAMAMNEH – ABUANZEH, 2023 = ALRAMAMNEH, I. M. – ABUANZEH, A.: International and National Procedural Framework for Combating Cybercrime. International Journal of Cyber Criminology, Vol. 17, No. 2, 2023, pp. 330–349.

15- AL-RAZOUQ – AL-ADAYLEH, 2023 = AL-RAZOUQ, T. – AL-ADAYLEH, B.: Documenting Emergency Law: Jordan's Response to the COVID-19 Pandemic. Raghadan Journal, Vol. 1, No. 1, 2023, pp. 81–100.

16- ALSHARIF et al., 2022 = ALSHARIF, M. – MISHRA, S. – ALSHEHRI, M.: Impact of Human Vulnerabilities on Cybersecurity. Computer Systems Science and Engineering, Vol. 40, No. 3, 2022, pp. 1153–1166. https://doi.org/10.32604/csse.2022.019938.

17- ALSOBEH et al., 2023 = ALSOBEH, A. – ALAZZAM, I. – SHATNAWI, A. – KHASAWNEH, I.: Cybersecurity Awareness Factors among Adolescents in Jordan: Mediation Effect of Cyber Scale and Personal Factors. Online Journal of Communication and Media Technologies, Vol. 13, No. 2, 2023, Article e202312, pp. 1–20.

18- ANSARI et al., 2022 = ANSARI, Meraj Farheen – DASH, Bibhu – SHARMA, Pawankumar – YATHIRAJU, Nikhitha: The Impact and Limitations of Artificial

Intelligence in Cybersecurity: A Literature Review. International Journal of Advanced Research in Computer and Communication Engineering, Vol. 11, No. 9, 2022, pp. 81–91.

19- ARROYABE et al., 2024 = ARROYABE, Marta F. – ARRANZ, Carlos F. A. – FERNANDEZ DE ARROYABE, Ignacio – FERNANDEZ DE ARROYABE, Juan Carlos: Exploring the Economic Role of Cybersecurity in SMEs: A Case Study of the UK. Technology in Society, Vol. 78, 2024, Article 102670, pp. 1–10. DOI: 10.1016/j.techsoc.2024.102670.

20- ASLAN et al., 2023 = ASLAN, Ö. – AKTUĞ, S. S. – OZKAN-OKAY, M. – YILMAZ, A. A. – AKIN, E.: A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, Vol. 12, No. 6, 2023, Article 1333, pp. 1–42.

21- AUSTIN, 2020 = AUSTIN, B. T.: Nullum Crimen, Nulla Poena Sine Lege: The Principle of Penal Legality in the Ius Vigens. Studia Canonica, Vol. 54, 2020, pp. 5–29. https://doi.org/10.2143/STC.54.1.3288465.

22- BLACK – BALDWIN, 2012 = BLACK, Julia – BALDWIN, Robert: When Risk-Based Regulation Aims Low: Approaches and Challenges. Regulation & Governance, Vol. 6, No. 1, 2012, pp. 2–22. https://doi.org/10.1111/j.1748-5991.2011.01124.x.

23- BURRI – ZIHLMANN, 2023 = BURRI, M. – ZIHLMANN, Z.: The EU Cyber Resilience Act – An Appraisal and Contextualization. EuZ Zeitschrift für Europarecht, 2023, pp. B1–B42.

24- BUSETTI – SCANNI, 2024 = BUSETTI, Simone – SCANNI, Francesco Maria: Evaluating Incident Reporting in Cybersecurity: From Threat Detection to Policy Learning. Government Information Quarterly, Vol. 42, No. 1, 2024, Article 102000, pp. 1–12. https://doi.org/10.1016/j.giq.2024.102000.

25- BUTTIGIEG – BRUNELLI, 2024 = BUTTIGIEG, Christopher P. – BRUNELLI ZIMMERMANN, Beatriz: The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of Europe's Architecture for Financial Supervision. ERA Forum, Vol. 25, Springer, 2024, pp. 11–28.

26- BYGRAVE, 2022 = BYGRAVE, L. A.: Security by Design: Aspirations and Realities in a Regulatory Context. Oslo Law Review, Vol. 8, No. 3, 2022, pp. 126–177.

27- CASTALDO – SERINI, 2024 = CASTALDO, Francesca – SERINI, Federico: Public-Private Collaboration in European Cybersecurity. Between Organizational and Regulatory

Plans. Teoria e Critica della Regolazione Sociale / Theory and Criticism of Social Regulation, Vol. 2, No. 29, 2024, pp. 177–194. DOI: 10.7413/197054760154.

28- CATE et al., 2017 = CATE, Fred H. – KUNER, Christopher – SVANTESSON, Dan Jerker B. – LYNSKEY, Orla – MILLARD, Christopher: The Rise of Cybersecurity and Its Impact on Data Protection. International Data Privacy Law, Vol. 7, No. 2, 2017, pp. 73–75.

29- CHAŁUBIŃSKA – NOWIKOWSKA, 2024 = CHAŁUBIŃSKA-JENTKIEWICZ, K. – NOWIKOWSKA, M.: Entities Involved in the Policy of Ensuring the Security of Network and Information Systems in the Light of the NIS 2 Directive (Part 1). Cybersecurity and Law, Vol. 11, No. 1, 2024, pp. 5–20. DOI: 10.35467/cal/187253.

30- CHIARA, 2022 = CHIARA, Pier Giorgio: The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements. International Cybersecurity Law Review, Vol. 3, 2022, pp. 255–273.

31- CHIARA, 2025 = CHIARA, Pier Giorgio: Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise? European Journal of Risk Regulation, Vol. 16, No. 2, 2025, pp. 469–484. DOI: 10.1017/err.2025.9.

32- CHNG et al., 2022 = CHNG, S. – LU, H. Y. – KUMAR, A. – YAU, D.: Hacker Types, Motivations and Strategies: A Comprehensive Framework. Computers in Human Behavior Reports, Vol. 5, 2022, Article 100167, pp. 1–8.

33- COTTA – RIGHETTINI, 2026 = Cotta, Benedetta – Righettini, Maria Stella: Governing Cybersecurity in the Digital Age: Mapping Comprehensive Policy Mixes with the Nodality-Authority-Treasure-Organization Lens. Review of Policy Research, Vol. 43, No. 4, 2026, pp. 1-15 Article e70113. DOI: 10.1111/ropr.70113

34- CREMER et al., 2022 = Cremer, F. – Sheehan, B. – Fortmann, M. – Kia, A. N. – Mullins, M. – Murphy, F. – Materne, S.: Cyber Risk and Cybersecurity: A Systematic Review of Data Availability. The Geneva Papers on Risk and Insurance – Issues and Practice, Vol. 47, No. 3, 2022, pp. 698–736. DOI: 10.1057/s41288-022-00266-6.

35- CULOT et al., 2021 = CULOT, Giovanna – NASSIMBENI, Guido – PODRECCA, Matteo – SARTOR, Marco: The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory-Based Research Agenda. The TQM Journal, Vol. 33, No. 7, 2021, pp. 76–105. DOI: 10.1108/TQM-09-2020-0202.

36- DEWI – NUGRAHANI, 2024 = DEWI, Arie Setya – NUGRAHANI, Henny Saptatia Drajati: Strengthening EU Cyber Resilience: A Critical Analysis of the Cyber Solidarity Act's Legislative Framework. Journal of Islamic World and Politics, Vol. 8, No. 2, 2024, pp. 182–195.

37- DE-YOLANDE et al., 2023 = DE-YOLANDE, M. – DOH-DJANHOUNDJI, T. – CONSTANT, G.: Breach Notification in the General Data Protection Regulation. Voice of the Publisher, Vol. 9, 2023, pp. 334–347. https://doi.org/10.4236/vp.2023.94026.

38- Efe – Bengshir, 2019 = Efe, Ahmet – Bengshir Kaya: Innovation in the Governance Paradigm from IT Governance to Good Enough Governance. Yönetim Bilişim Sistemleri Dergisi, Vol. 5, No. 1, 2019, pp. 31–51.

39- FERGUSON, 2022 = FERGUSON, D. D. S.: European Cybersecurity Certification Schemes and Cybersecurity in the EU Internal Market. International Cybersecurity Law Review, Vol. 3, 2022, pp. 51–114. DOI: 10.1365/s43439-021-00044-5.

40- GHOSH, 2022 = GHOSH, U.: Cyber Security Issues by Using the Internet of Things (IoT) – A Legal Analysis. Indian Journal of Law and Legal Research, Vol. 4, No. 4, 2022, pp. 1–16.

41- GOLDSTEIN, 2019 = GOLDSTEIN, K.: Cyber Beware: IoT Technology Growing Explosively. International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel, Vol. 3, No. 6, 2019, pp. 7–13.

42- HESSEL – REBMANN, 2020 = HESSEL, Stefan – REBMANN, Andreas: Regulation of Internet-of-Things Cybersecurity in Europe and Germany as Exemplified by Devices for Children. International Cybersecurity Law Review, Vol. 1, No. 1, 2020, pp. 27–37. https://doi.org/10.1365/s43439-020-00006-3.

43- HOLZENBERGER – MAXWELL, 2025 = HOLZENBERGER, Nils – MAXWELL, Winston: A Quantitative Approach to the GDPR's Anonymisation and "Appropriate Technical and Organisational Measures" Tests. Computer Law & Security Review, Vol. 59, 2025, Article 106173, pp. 1–13. https://doi.org/10.1016/j.clsr.2025.106173.

44- HOSSAIN, 2023 = HOSSAIN, Bayazid: Digital Evidence in Foreign Jurisdiction and Quality of Justice. ELCOP Journal on Human Rights, Vol. 1, No. 1, 2023, pp. 143–159. DOI: 10.59871/SFGB7594.

45- JOSWIG – KURZ, 2025 = JOSWIG, Thomas – KURZ, Walter: Empirical Analysis of NIS2 Adoption in EU SMEs: Challenges for Critical Infrastructure in Germany. Journal of Next-Generation Research 5.0 (JNGR 5.0), Vol. 1, No. 3, 2025, pp. 1–21.

46- KHURSHID et al., 2022 = KHURSHID, A. – ALSAAIDI, R. – ASLAM, M. – RAZA, S.: EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme. IEEE Access, Vol. 10, 2022, pp. 129932–129948. DOI: 10.1109/ACCESS.2022.3225973.

47- KHWAILEH, 2025 = KHWAILEH, Khaled Mohammad: Public Perceptions of Jordan's Cybercrime Law: Protecting Social Media Data and Aligning with International Standards. Pakistan Journal of Life and Social Sciences, Vol. 23, No. 1, 2025, pp. 2947–2955.

48- KOHLER, 2020 = KOHLER, C.: The EU Cybersecurity Act and European Standards: An Introduction to the Role of European Standardization. International Cybersecurity Law Review, Vol. 1, 2020, pp. 7–12. DOI: 10.1365/s43439-020-00008-1.

49- KOSIŃSKI et al., 2018 = KOSIŃSKI, J. – KOŚLA, R. – GONTARZ, T.: Cybersecurity and the Handling of Cyber Incidents. Internal Security, Vol. 10, 2018, pp. 107–128. https://doi.org/10.5604/01.3001.0013.4219.

50- LALLIE et al., 2021 = LALLIE, H. S. – SHEPHERD, L. A. – NURSE, J. R. C. – EROLA, A. – EPIPHANIOU, G. – MAPLE, C. – BELLEKENS, X.: Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic. Computers & Security, Vol. 105, 2021, Article 102248, pp. 1–20. https://doi.org/10.1016/j.cose.2021.102248.

51- LOTFI, 2022 = LOTFI, W.: International Efforts in Combating Cyberterrorism Crimes. Journal of the Faculty of Economics and Political Science, Cairo University, Vol. 23, No. 1, 2022, pp. 151–178.

52- MICHELS – WALDEN, 2020 = MICHELS, Johan David – WALDEN, Ian: Beyond ‘Complacency and Panic’: Will the NIS Directive Deliver a Step Change in EU Cybersecurity? European Law Review, Vol. 45, No. 1, 2020, pp. 87–102.

53- MOSTAFA, 2022 = MOSTAFA, Islam: The Crime of Breaching Cybersecurity and the Protection of the Use of Data and Information under Egyptian Law. Al-Majalla Al-Qanuniyya (Legal Journal), Vol. 12, No. 2, 2022, pp. 718–754.

54- MOURAD, 2025 = MOURAD, Yourmeche: The Legal Nature of Cybercrime. Journal of Legal Studies and Researches, Vol. 10, No. 2, 2025, pp. 27–42.

55- NAGYFEJEO – VON SOLMS, 2020 = NAGYFEJEO, Eva – VON SOLMS, Basie: Why Do National Cybersecurity Awareness Programmes Often Fail? International Journal of Information Security and Cybercrime, Vol. 9, No. 2, 2020, pp. 18–27. DOI: 10.19107/IJISC.2020.02.03.

56- OPDERBECK, 2016 = OPDERBECK, David W.: Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry. Maryland Law Review, Vol. 75, No. 4, 2016, pp. 935–983.

57- ORTEGA VELÁZQUEZ et al., 2025 = ORTEGA VELÁZQUEZ, M. Á. – CUEVAS MARTÍNEZ, I. – JARA, A. J.: Integrating the CRA into the IoT Lifecycle: Challenges, Strategies, and Best Practices. Information, Vol. 16, No. 12, 2025, Article 1017, pp. 1–28. https://doi.org/10.3390/info16121017.

58- PAULOVICS – ALBUSTANJI, 2026 = PAULOVICS, Anita – ALBUSTANJI, Huthaifa: A Critical Review of The Jordanian Legal Frameworks on International Cooperation in Combating Cybercrime. AAU Journal of Business and Law, Vol. 10, No. 1, 2026, pp. 24–42. DOI: 10.51958/AAUJBL2026V10I1P7.

59- PHILLIPS et al., 2022 = PHILLIPS, K. – DAVIDSON, J. C. – FARR, R. R. – BURKHARDT, C. – CANEPPELE, S. – AIKEN, M. P.: Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, Vol. 2, No. 2, 2022, pp. 379–398.

60- PORZEŻYŃSKI – KULICKI, 2024 = PORZEŻYŃSKI, M. – KULICKI, Ł.: Changes Introduced by the NIS Directive 2.0 and Their Potential Effect on Shaping the Cybersecurity Labour Market. Cybersecurity and Law, Vol. 11, No. 1, 2024, pp. 21–38. DOI: 10.35467/cal/187254.

61- RISWALDI, 2025 = RISWALDI, Indra Lutrian: Legal Problems of Personal Data Protection in The Digital Era in Personal Data Protection Law in Indonesia. Greenation International Journal of Law and Social Sciences, Vol. 3, No. 2, 2025, pp. 345–350. https://doi.org/10.38035/gijlss.v3i2.429.

62- SAŁEK – FAJDEK, 2025 = SAŁEK, Konrad – FAJDEK, Patryk: Analysis of the Implementation of the NIS2 Directive in the Weimar Triangle Countries. Central European

Review of Economics & Finance, Vol. 50, No. 1, 2025, pp. 41–52. DOI: 10.24136/ceref.2025.003.

63- SALEOUS et al., 2023 = SALEOUS, H. – ISMAIL, M. – ALDAAJEH, S. H. – MADATHIL, N. – ALRABAEE, S. – CHOO, K.-K. R. – AL-QIRIM, N.: COVID-19 Pandemic and the Cyber Threat Landscape: Research Challenges and Opportunities. Digital Communications and Networks, Vol. 9, No. 1, 2023, pp. 211–222.

64- SÁNTHA – ALBUSTANJI, 2025 = SÁNTHA, Ferenc – ALBUSTANJI, Huthaifa: Cyber Aggression Crimes: A Comparative Study of the Jordanian and the Hungarian Legal Frameworks. Publicationes Universitatis Miskolcinensis, Sectio Juridica et Politica, Tomus XLIII, 2025, pp. 220–251.

65- SARKAR – SHUKLA, 2024 = SARKAR, G. – SHUKLA, S. K.: Reconceptualizing Online Offenses: A Framework for Distinguishing Cybercrime, Cyberattacks, and Cyberterrorism in the Indian Legal Context. Journal of Economic Criminology, Vol. 4, 2024, Article 100063, pp. 1–17.

66- SCHMITZ-BERNDT – CHIARA, 2022 = SCHMITZ-BERNDT, Sandra – CHIARA, Pier Giorgio: One Step Ahead: Mapping the Italian and German Cybersecurity Laws Against the Proposal for a NIS2 Directive. International Cybersecurity Law Review, Vol. 3, 2022, pp. 289–311.

67- SCHMITZ-BERNDT – COLE, 2022 = SCHMITZ-BERNDT, Sandra – COLE, M. D.: Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act. ACIG, Vol. 1, No. 1, 2022, pp. 1–17. DOI: 10.5604/01.3001.0016.132.

68- SCHMITZ-BERNDT, 2023 = SCHMITZ-BERNDT, Sandra: Defining the Reporting Threshold for a Cybersecurity Incident Under the NIS Directive and the NIS 2 Directive. Journal of Cybersecurity, Vol. 9, No. 1, 2023, Article tyad009, pp. 1–13. https://doi.org/10.1093/cybsec/tyad009.

69- SEN, 2023 = SEN, Nicholas: Cybersecurity Incident Reporting Laws in the Asia Pacific. International Cybersecurity Law Review, Vol. 4, 2023, pp. 325–346.

70- SHAFFIQUE, 2024 = SHAFFIQUE, Mohammed Raiz: Cyber Resilience Act 2022: A Silver Bullet for Cybersecurity of IoT Devices or a Shot in the Dark? Computer Law &

Security Review, Vol. 54, 2024, Article 106009, pp. 1–15. DOI: 10.1016/j.clsr.2024.106009.

71- SINGH, 2022 = SINGH, Lawanya: Cyber Crime, Cyber Resilience and Security Strategy in Post-Pandemic World. Supremo Amicus, Vol. 28, 2022, pp. 305–317.

72- SINROD – REILLY, 2000 = SINROD, Eric J. – REILLY, William P.: Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws. Santa Clara Computer and High Technology Law Journal, Vol. 16, No. 2, 2000, pp. 1–50.

73- SMIRNOVA – TRAVIESO-MORALES, 2024 = SMIRNOVA, Yelena – TRAVIESO-MORALES, Victoriano: Understanding Challenges of GDPR Implementation in Business Enterprises: A Systematic Literature Review. International Journal of Law and Management, Vol. 66, No. 3, 2024, pp. 326–344. https://doi.org/10.1108/IJLMA-08-2023-0170.

74- SPIEKERMANN, 2012 = SPIEKERMANN, Sarah: The Challenges of Privacy by Design. Communications of the ACM, Vol. 55, No. 7, 2012, pp. 38–40. https://doi.org/10.1145/2209249.2209263.

75- SVIATUN et al., 2021 = SVIATUN, O. V. – GONCHARUK, O. V. – ROMAN, C. – KUZMENKO, O. – KOZYCH, I. V.: Combating Cybercrime: Economic and Legal Aspects. WSEAS Transactions on Business and Economics, Vol. 18, 2021, pp. 751–762.

76- TAHMASEBI, 2024 = TAHMASEBI, Meysam: Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises. Journal of Information Security, Vol. 15, No. 2, 2024, pp. 106–133.

77- TEICHMANN, 2025 = TEICHMANN, Fabian: Cybersecurity of Critical Infrastructure in Europe: The NIS2 Directive in Focus. International Cybersecurity Law Review, Vol. 6, 2025, pp. 207–220.

78- TEICHMANN, 2026 = TEICHMANN, Fabian: The Cyber Resilience Act as a New Paradigm for Product Security: A Compliance Roadmap. International Cybersecurity Law Review, Vol. 7, 2026, pp. 1–17. https://doi.org/10.1365/s43439-025-00162-4.

79- THIWISHA – VANITHA, 2026 = Thiwisha, M. S. – Vanitha, P.: A Research Paper on Cyber Security Threats and Challenges. International Journal of Science, Strategic Management and Technology, Vol. 2, No. 3, March 2026, pp.1-9.

80- VALKENBURG – BONGIOVANNI, 2024 = VALKENBURG, Bert – BONGIOVANNI, Ivano: Unravelling the Three Lines Model in Cybersecurity: A Systematic Literature Review. Computers & Security, Vol. 139, 2024, Article 103708, pp. 2–11. https://doi.org/10.1016/j.cose.2024.103708.

81- VANDEZANDE, 2024 = VANDEZANDE, Niels: Cybersecurity in the EU: How the NIS2 Directive Stacks Up Against Its Predecessor. Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 52, 2024, pp. 1–16. Available at: https://ssrn.com/abstract=4383118 (Accessed: 11 November 2025).

82- VILLANI, 2025 = VILLANI, Susanna: The Cyber Solidarity Act: Framework and Perspectives for the New EU-Wide Cybersecurity Solidarity Mechanism Under the EU Legal System. European Journal of Risk Regulation, Vol. 16, No. 2, 2025, pp. 485–497. DOI: 10.1017/err.2025.24.

83- WAH – ZUREIGAT, 2025 = WAH, Khaw Khai – ZUREIGAT, Mohammad Rafiq: The Role of Cybersecurity Governance in Enhancing the Sustainability of Jordanian Financial Institutions: Strategies and Trends. International Journal of Academic Research in Business and Social Sciences, Vol. 15, No. 4, 2025, pp. 1038–1057.

84- WAQDAN et al., 2025 = WAQDAN, Mofareh – LOUAFI, Habib – MOUHOUB, Malek: Security Risk Assessment in IoT Environments: A Taxonomy and Survey. Computers & Security, Vol. 154, 2025, Article 104456, pp. 1–16. https://doi.org/10.1016/j.cose.2025.104456.

85- WELUKAR – BAJORIA, 2021 = WELUKAR, Jenis – BAJORIA, Gagan: Artificial Intelligence in Cyber Security – A Review. International Journal of Scientific Research in Science and Technology, Vol. 8, No. 6, 2021, pp. 488–491.

86- YOUNES et al., 2024 = YOUNES, Alaa Majed Ahmad Bani – AL-RAWASHED, Ammar Mahmoud Ayoub – AL RASHDAN, Aseel Mahmoud – ALBTOOSH, Ahmad Fahed Mohammad: Legislative Evolution of Cyber Security in Jordanian Law. Migration Letters, Vol. 21, No. S4, 2024, pp. 816–828.

87- ZAMFIROIU – SHARMA, 2022 = ZAMFIROIU, Alin – SHARMA, Ramesh C.: Cybersecurity Management for Incident Response. Romanian Cyber Security Journal, Vol. 4, No. 1, 2022, pp. 69–75. https://doi.org/10.54851/v4i1y202208.

Books

1- KOTT – LINKOV, 2019 = KOTT, A. – LINKOV, I. (eds): Cyber Resilience of Systems and Networks. Risk, Systems and Decisions. Springer, Cham, 2019, pp. 1–475. DOI: 10.1007/978-3-319-77492-3.
2- MUECK – GAIE, 2025 = MUECK, M. – GAIE, C. (eds): European Digital Regulations. Intelligent Systems Reference Library, Vol. 265. Springer, Cham, 2025, pp. 1–245. DOI: 10.1007/978-3-031-80809-8.
3- NAMOUR, 2024 = NAMOUR, Mohammad Saeed: Principles of Criminal Procedure. 6th ed. Dar Al-Thaqafa for Publishing and Distribution, Amman, 2024, pp. 1–712.
4- WIENER, 1961 = WIENER, Norbert: Cybernetics: Or Control and Communication in the Animal and the Machine. 2nd revised edn. Hermann & Cie – MIT Press, Cambridge, 1961, pp. 1–231.

Book Chapter

1- BADA – NURSE, 2020 = BADA, M. – NURSE, J. R. C.: The Social and Psychological Impact of Cyberattacks. In: Emerging Cyber Threats and Cognitive Vulnerabilities. (eds: BENSON, V. – MCALANEY, J.) Academic Press, 2020, pp. 73–92
2- GAIE – MUECK, 2025 = GAIE, C. – MUECK, M.: Introduction to the Networks and Information Systems 2 (NIS2) Directive. In: European Digital Regulations. (eds: MUECK, M. – GAIE, C.) Intelligent Systems Reference Library, Vol. 265. Springer, Cham, 2025, pp. 161–180. DOI: 10.1007/978-3-031-80809-8_7.
3- SÁNTHA, 2024 = SÁNTHA, Ferenc: Definition and Systematisation of Cybercrimes. In: Cybercrime. (ed.: GRYSZCZYŃSKA, Agnieszka) Wydawnictwo Instytutu Wymiaru Sprawiedliwości, Warsaw, 2024, pp. 27–44. DOI: 10.32041/9788367149761/1.
4- WEIPPL – SCHRITTWIESER, 2024 = WEIPPL, E. – SCHRITTWIESER, S.: Introduction to Security and Privacy. In: Introduction to Digital Humanism. (eds: WERTHNER, H. et al.) Springer, Cham, 2024, pp. 397–414. https://doi.org/10.1007/978-3-031-45304-5_26 (Accessed: 13 September 2025).

Conference proceedings

1- ASLAN, 2016 = ASLAN, Ö.: How to Decrease Cyber Threats by Reducing Software Vulnerabilities and Bugs. In: Proceedings of the 1st International Mediterranean Science

and Engineering Congress, Çukurova University, Adana, Turkey, 26–28 October 2016, pp. 639–646.

2- BUCHMANN – HARTMANN, 2020 = BUCHMANN, E. – HARTMANN, A.: Identifying Long-Term Risks of the Internet of Things. In: UBICOMM 2020: The 14th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, 2020, pp. 47–50.

3- KUZMINYKH et al., 2022 = KUZMINYKH, I. – GHITA, B. – SUCH, J. M.: The Challenges with Internet of Things Security for Business. In: Internet of Things, Smart Spaces, and Next Generation Networks and Systems. (eds: KOUCHERYAVY, Y. – BALANDIN, S. – ANDREEV, S.) Lecture Notes in Computer Science, Vol. 13158. Springer, Cham, 2022, pp. 46–58. https://doi.org/10.1007/978-3-030-97777-1_5.

Master Thesis

GIANNAKOULIAS, 2023 = GIANNAKOULIAS, Alkiviadis: NIS 2 Directive: Implications for System and Infrastructure Security. Master's thesis. University of Piraeus, 2023, pp. 1–54.

Professional / Practitioner Publications

WEBBER – TAYLOR, 2016 = WEBBER, Mark – TAYLOR, Stuart: The NIS Directive – A Practical Perspective. Privacy & Data Protection (P. & D.P.), Vol. 16, No. 3, 2016, pp. 9–12.

Statutes, Regulations, and Official Legal Acts:

European Union Legislation and Official Reports:

1- Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence CETS No. 224, 2022. Available at https://rm.coe.int/1680a49dab?utm (Accessed: 19 September 2026).

2- Council of Europe: Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (ETS No. 189), Strasbourg, 28 January 2003. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 (Accessed: 4 September 2025).

3- Council of Europe: Convention on Cybercrime (ETS No. 185, Budapest Convention), Budapest, 23 November 2001. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (Accessed: 4 September 2025).
4- European Commission, Impact Assessment Report Accompanying the Proposal for a Directive on Measures for a High Common Level of Cybersecurity Across the Union, Repealing Directive (EU) 2016/1148, SWD (2020) 345 final, Brussels, 16 December 2020, pp. 1–96.
5- European Commission, Impact Assessment Report Accompanying the Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020, SWD(2022) 282 final, Brussels, 15 September 2022.
6- European Commission: Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for the application of Directive (EU) 2016/1148 as regards further specification of the elements to be taken into account by digital service providers and parameters for determining substantial incident impact, Official Journal of the European Union, L 26, 31 January 2018, pp. 48–51.
7- European Parliament and Council of the European Union, Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities, L 281, 23 November 1995, pp. 31–50.
8- European Parliament and Council of the European Union, Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), Official Journal of the European Union, L 194, 19 July 2016, pp. 1–30.
9- European Parliament and Council of the European Union, Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Official Journal of the European Union, L 334, 27 December 2022, pp. 80–152.
10- European Parliament and Council of the European Union, Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities (CER Directive), Official Journal of the European Union, L 333, 27 December 2022, pp. 164–197.

11- European Parliament and Council of the European Union, Regulation (EC) No. 460/2004 of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance), Official Journal of the European Union, L 77, 13 March 2004, pp. 1–11.
12- European Parliament and Council of the European Union, Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L 119, 4 May 2016, pp. 1–88.
13- European Parliament and Council of the European Union, Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Official Journal of the European Union, L 151, 7 June 2019, pp. 15–69.
14- European Parliament and Council of the European Union, Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA), Official Journal of the European Union, L 333, 27 December 2022, pp. 1–79.
15- European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), Official Journal of the European Union, L 2024/1689, 12 July 2024.
16- European Parliament and Council of the European Union, Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), Official Journal of the European Union, L 2024/2847, 20 November 2024, pp. 1–81.
17- European Parliament and Council of the European Union, Regulation (EU) 2025/38 of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), Official Journal of the European Union, L 2025/38, 15 January 2025, pp. 1–34.
18- European Parliament and of the Council, Regulation (EU) 2026/1744 of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards

the simplification of the implementation of harmonized rules on artificial intelligence (Digital Omnibus on AI).

Jordanian Legislation:

1- Jordan, Administrative Organization Regulation of the National Cybersecurity Center No. 25 of 2021, Official Gazette No. 5721, 1 June 2021, p.2006.
2- Jordan, Criminal Law No. 16 of 1960, Official Gazette No. 1487, 1 May 1960, p. 374.
3- Jordan, Criminal Procedure Law No. 9 of 1961 and its amendments, Official Gazette No. 1539, 16 March 1961, p. 311.
4- Jordan, Cybersecurity Law No. 16 of 2019, Official Gazette No. 5595, 16 September 2019, p. 5143.
5- Jordan, Cybersecurity Service Providers Licensing Regulation No. 76 of 2024, Official Gazette No. 5962, 17 November 2024, p. 6429.
6- Jordan, Defense Law No. 13 of 1992, Official Gazette No. 3815, 25 March 1992, p. 586.
7- Jordan, Economic Crimes Law No. 11 of 1993, Official Gazette No. 3891, 17 April 1993, p. 722.
8- Jordan, Electronic Crimes Law No. 17 of 2023, Official Gazette No. 5874, 13 August 2023, p. 3579.
9- Jordan, Electronic Crimes Law No. 27 of 2015, Official Gazette No. 5343, 1 June 2015, p. 5631.
10- Jordan, Instructions for Determining the Criteria for Violations of the Provisions of the Cybersecurity Law, Their Controls and the Procedures Due Thereto for the Year 2025, Official Gazette No. 5984, 3 April 2025, p. 1871.
11- Jordan, National Cybersecurity Center Regulation No. 1 of 2020, Official Gazette No. 5614, 2 January 2020, p. 1.
12- Jordan, Personal Data Protection Law No. 24 of 2023, Official Gazette No. 5881, 17 September 2023, p. 4338.
13- Jordan, Temporary Information Systems Crimes Law No. 30 of 2010, Official Gazette No. 5056, 16 September 2010, p. 5334.
14- Jordan, The Constitution of the Hashemite Kingdom of Jordan of 1952, Official Gazette No. 1093, 8 January 1952, p. 3 (as amended up to Official Gazette No. 5770, 31 January 2022).

Other National Legislation:

1- Belgium: Act of 7 April 2019 on the Security of Network and Information Systems, Moniteur Belge / Belgisch Staatsblad, 3 May 2019.
2- Germany, Bundesamt für Sicherheit in der Informationstechnik-Gesetz (BSIG) as amended by the NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (2025), Bundesgesetzblatt [BGBl] I, 2 December 2025, No. 301, p. 2. Available at: https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html. (Accessed 26 September 2026).
3- Hungary, Act CXXXV of 2025 on the Implementation of the European Union Cyber Resilience Regulation in Hungary and the Amendment of Certain Cybersecurity Provisions. Hungarian Gazette (Magyar Közlöny), No. 158, 29 December 2025. Available at https://magyarkozlony.hu/dokumentumok/adbf9bdb4753d3f6e020f3486f3a3e3ff734cb9e/megtekintes (Accessed 4 July 2026).
4- State of Qatar, Amiri Decision No. 1 of 2021 Establishing the National Cyber Security Agency, Official Gazette of the State of Qatar, Issue No. 3, 7 February 2021.
5- United States of America: Food Safety Modernization Act, Pub. L. No. 111-353, 124 Stat. 3885 (2011).

Judicial Decisions and Case Law:

1- Jordan, North Amman Magistrate Court (Criminal): Decision No. 6558/2018, Judgment of 15 June 2018.
2- Jordan, Irbid Magistrate Court (Criminal): Decision No. 6259/2022, Judgment of 8 May 2023.
3- Jordan, Amman Court of First Instance (Criminal Division, Appellate Jurisdiction), Decision No. 1050/2021, Judgement of 9 May 2021.
4- Jordan, Amman Court of First Instance (Criminal Division, Appellate Jurisdiction), Decision No. 6267/2018, Judgment of 8 November 2018.

Annex 1: Supervisors Evaluation and Recommendations

Supervisor's Evaluation and Recommendation Workshop Discussion

I. Administrative and Dissertation Details

- **Name of Doctoral Candidate:** Huthaifa Mohammad Ahmad Albustanji
- **Doctoral School**: Ferenc Deák Doctoral School of Law, University of Miskolc
- **Title of Doctoral Dissertation:** The Legal Governance of Cybersecurity: A Critical Comparative Analysis of the European Union and Jordan
- **Organizational Unit:** Institute of Criminal Sciences, Faculty of Law, University of Miskolc
- **Supervisors:**
  - Prof. Dr. Anita Paulovics, Full Professor, Vice-Dean
  - Dr. Ferenc Sántha, Associate Professor

II. Evaluation of the Research and Dissertation Manuscript

The doctoral dissertation submitted by Mr. Huthaifa Mohammad Ahmad Albustanji examines a highly topical and rapidly evolving area of contemporary legal scholarship: the legal governance of cybersecurity through a critical comparative analysis of the European Union and the Hashemite Kingdom of Jordan.

During his doctoral studies, the candidate has demonstrated a high degree of academic commitment, research independence, and analytical competence. The dissertation develops a comprehensive legal framework for examining cybersecurity governance by bringing together two complementary dimensions of legal regulation: the ex post criminal-law response to unlawful cyber conduct and the ex ante administrative and regulatory mechanisms designed to prevent, manage, and mitigate cybersecurity risks.

The dissertation provides a systematic examination of the principal European Union cybersecurity instruments, including, in particular, Directive (EU) 2022/2555 (NIS2 Directive), Regulation (EU) 2024/2847 (Cyber Resilience Act), and related regulatory instruments, and critically compares them with the developing Jordanian cybersecurity framework, including Cybersecurity Law No. 16 of 2019, Electronic Crimes Law No. 17 of 2023, and relevant administrative and regulatory developments.

Particular value is placed on the dissertation's identification of structural and functional differences between the two legal systems, including differences in regulatory scope, institutional responsibility, risk-based regulation, enforcement mechanisms, private-sector obligations, and the

continuity of cybersecurity governance across the prevention, preparedness, response, and recovery stages.

On this comparative basis, the candidate formulates a coherent set of legal and regulatory reform proposals for Jordan, while also identifying broader implications for the development of effective cybersecurity governance in contemporary digital societies. The dissertation therefore combines doctrinal legal analysis with a comparative and reform-oriented approach.

The research methodology is appropriate to the objectives of the dissertation and is applied in a systematic manner. The relevant legislation, regulatory instruments, academic literature, and institutional materials have been examined extensively, with due attention to the continuing development of the field. The dissertation demonstrates the candidate's capacity to analyze complex and technically informed legal questions within a coherent doctrinal and comparative framework. The manuscript is supported by appropriate academic references and complies with the applicable requirements concerning scholarly documentation and citation.

III. Formal Recommendation

Having considered the scientific quality, originality, methodological soundness, comparative contribution, and formal completeness of the dissertation, we consider the manuscript sufficiently developed to proceed to the workshop discussion.

1- Prof. Dr. Anita Paulovics

Supervisor Miskolc, 10 September 2026

2- Dr. Ferenc Sántha

Co-Supervisor Miskolc, September 2026

Scanned with CamScanner

Annex 2: Researcher's Publications During Study Period (2023-2026)

1- ALBUSTANJI, H. M.: Jurisdiction of Cyber-threats in the Context of International Law. In: Crisis, economy, technology and law: Conference Proceedings – Selected Studies, 2023. https://publicatio.bibl.u-szeged.hu/30780/1/Nguyen.pdf

2- ALBUSTANJI, H. M.: COVID-19 Pandemic Impacts on Cyberattacks. In: International Scientific Conference »HEARD - The impact of COVID-19 crisis on diverse democratic perspectives through gender perspective«, 2024. https://www.researchgate.net/publication/385717187_COVID-19_Pandemic_Impacts_on_Cyberattacks

3- ALBUSTANJI, H. M.: New EU Cybersecurity Legislation Challenges and Ramifications. Conference Proceedings, Hungarian National Scientific Bibliography (MTMT ID: 35728023), 2024. https://www.researchgate.net/publication/385717283_New_EU_Cybersecurity_Legislation_Challenges_and_Ramifications?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6ImhvbWUiLCJwYWdlIjoicHJvZmlsZSIsInBvc2l0aW9uIjoicGFnZUNvbnRlbnQifX0.

4- ALBUSTANJI, H. M. – PAULOVICS, A.: A Critical Review of The Jordanian Legal Frameworks on International Cooperation in Combating Cybercrime. AAU Journal of Business and Law, Vol. 10, No. 1, 2025. https://journal.aau.ac.ae/files/1770016710_full_article.pdf.

5- ALBUSTANJI, H. M.: Using AI in Cybersecurity Within the European Union: - Double Edge Sword. Revista Facultății de Drept Oradea, No. 2, 2023 [published April 2025]. https://www.ceeol.com/search/article-detail?id=1329026.

6- SÁNTHA, F. – ALBUSTANJI, H. M.: Cyber aggression crimes: a comparative study of the Jordanian and the Hungarian legal frameworks. Publicationes Universitatis Miskolcinensis, Sectio Juridica et Politica, 2025. https://ojs.uni-miskolc.hu/index.php/juridicaetpolitica/article/view/4312.

7- ALBUSTANJI, H. M. A.: The Jordanian Legislative Policy for Cybersecurity Provisions between Reality and Aspirations. International Review of Law, Vol. 15, No. 1, 2026. https://journals.qu.edu.qa/index.php/IRL/article/view/6393 .

8- ALBUSTANJI, H.: Cybersecurity and Data Protection in the Age of IoT: A Comparative Legal Analysis in Jordan and the European Union. European Journal of Comparative Law and Governance, Vol. 14, No. 1, 2027.

Annex 3: AI Declaration

Statement

In accordance with the provisions of the Regulation on the Use of Artificial Intelligence of University of Miskolc and the Guidelines for the Use of Artificial Intelligence of the Deák Ferenc Doctoral School of Law, I, undersigned Huthaifa Mohammad Ahmad Albustanji (name), declare that I have used / have not used artificial intelligence in my doctoral dissertation and thesis booklets.

In the case of the use of artificial intelligence (hereinafter: AI), I declare the following:
1. The name of the AI tool used: Gemini (Google)
2. The URL and the version number of the AI tool used: https://gemini.google.com/
3. The exact date of production of the generated content (year, month, day):2025/2026
4. The purpose and extent of use (describing in detail which part of the dissertation and to what extent the use of AI affects, and for which sub-task the AI was used):
The AI tool was utilized exclusively for the linguistic proofreading, stylistic refinement, and lexical enhancement of the doctoral dissertation. Specifically, it was employed to elevate the academic register of the text by rephrasing select sentences with precise legal terminology and formal scholarly phrasing.

I acknowledge that according to the Guidelines for the Use of Artificial Intelligence of the Deák Ferenc Doctoral School of Law, *„The use of AI is prohibited for the formulation of theses, research results, conclusions, inferences and analyses. Any thesis or paper prepared in this way is not admissible."*

Miskolc, 2026, 09, 18

Huthaifa
signature