ONLINE ISSN: 3007-3197 | PRINT ISSN: 3007-3189

http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 5 (2025)

Cyber security Governance as a Pillar of Enterprise Risk Management: Designing a Compliance-Driven Framework for Operational Resilience, Policy Enforcement, and Regulatory Alignment

Dr Khawaja Tahir Mehmood[1], Zia Ashraf[2], Raza Iqbal[3], Adnan Ahmed Rafique[4], Hassam Gul[5], Muhammad Ali[6]

Article Details

Keywords: Cybersecurity governance, enterprise risk management, compliance, operational resilience, policy enforcement, regulatory alignment, risk maturity.

[1]Dr Khawaja Tahir Mehmood
Department of Electrical Engineering,
BZU Multan
Ktahir@bzu.edu.pk

[2]Zia Ashraf
College of Allied Health Professionals,
Government College University,
Faisalabad (38000), Pakistan.

[3]Raza Iqbal,
M.Phil. Scholar Computer Science,
National College of Business
Administration & Economics Multan
Campus Multan
ali.raza@bzu.edu.pk

[4]Adnan Ahmed Rafique
Assistant Professor, Department of CS
and IT, University of Poonch Rawalakot,
adnanrafique@upr.edu.pk

[5]Hassam Gul
International Islamic University,
Islamabad
hassamgulp@gmail.com

[6]Muhammad Ali
University of the Punjab
ali.qureshi1206@gmail.com

ABSTRACT

As cyber threats increase and regulations become more stringent, cybersecurity has become a fundamental component of ERM, making it imperative to move from peripheral reactive approaches to integrated compliance-based models. The current research focuses on the complicated incorporation of cybersecurity governance into ERM systems, including its operational use for strengthening established protection measures, implementation of policies, and compliance with international standards. The participants of the study consisted of 146 cybersecurity and risk management practitioners who responded to an online survey. These results show that the organizations that have well-developed governance programs, or those that have dedicated resources such as a CISO, risk reporting, as well as automation technologies in their organizational structure, can respond better during cyber incidents, have quickened response times and have higher levels of compliance to regulations. On the other hand, poor board level supervisory control, laser-like low usage of sophisticated automated tools and questionable compliance policies in hybrid work environments are areas of concern currently. This research fills the gap in the current literature by suggesting a compliance-based approach to organizing and managing cyber risk in the context of broader enterprise goals. The findings call for more attention to the issue of cybersecurity governance as essential not just as control but as a valuable resource for organizational sustainability and as a basis for risk-favourable decisions.

Introduction

Cybersecurity, which once was a technical-environment issue, is now a strategic governance problem for organizations that has significant implications on enterprise risk management (ERM). With the trend of digital transformation, cloud computing, and data-driven decision in organizations, the risk of cyber threats has become higher (Von Solms & Van Niekerk, 2013). Breaches, ransomware, and DoS attacks not only lead to the violation of information confidentiality but also interrupt business operations, erode stakeholders' trust, and cost hefty fines (ENISA, 2022; IBM Security, 2023).

ERM, typically an organization-wide program encompassing financial, operational, and strategic risks, is now being asked to include cyber risks within its realm. The COSO has recommended that cybersecurity should be integrated with ERM processes because the threats are ever-changing and organizations need to be ready for risk assessment and management (COSO, 2019). This mandates that a governance strategy that is strategic and also holistic be adopted by the organization, where cybersecurity is increased in scope and operational and compliance parameters throughout the organizational structure and not just limited to IT.

Cybersecurity governance refers to the regulation of the existing norms, duties, strategies, and other measures aimed at securing the usage of information systems and the alignment of such usage with the enterprise's goals (Posthumus & von Solms, 2004). Appropriate and effective governance structures involve assignments of responsibilities, risk management authorities, and controls, which remain key to effective management of risks in the long run. NIST identifies cybersecurity governance as a core function in their Cybersecurity Framework since it lays the basis for the identification, protection, detection, response and recovery processes required for organizations to be secure (NIST, 2018).

Hence, there is a disconnection between cybersecurity governance and other ERM frameworks as suggested by existing studies and case studies of cyber-attacks. Some organizations today address cybersecurity with an acute method, stressing on technical measures once an incident has occurred in preference to considering it as a framework for control and governance processes added to humanitarian risk management frameworks (Bada & Sasse, 2015). The case of Equifax in 2017 which involved a major incident such as the leakage of personal information of more than 145 million people and fines of $700 million are some of the effects of poor governance and lack of appropriate board control over cyber security measures (FTC, 2019). Likewise, the Colonial Pipeline ransomware attack in 2021 further proved that the critical sectors can be exposed to cyber threats without adequate governance frameworks that prevent ransomware attacks (GAO, 2021).

Due to the evolution of legal requirements, compliance is considered one of the drivers of cybersecurity governance. More recent enactments like the GDPR, CCPA, or sectorial ones like the HIPAA in the United States strengthen the standards of protection, communication of data breaches, and third-party accountability. This may result in either financial loss or a stain in the reputation of the firm as well as interruptions in operations (Greenleaf, 2018; Deloitte, 2021). Thus, a compliance-based approach can be viewed as quite useful for ensuring that cybersecurity activities correspond to the requirements of the existing legislation as well as the organization's risk management objectives.

However, there is no aggregate of models that clarify how cybersecurity governance can be integrated into ERM to influence compliance, enforcement of policy, and even resilience. Although there are formal guidelines such as ISO/IEC 27001 and COBIT 2019, they do not offer specific implementation approaches for various company types and sizes and different industries (ISACA, 2019; ISO/IEC, 2013). Therefore, research focused on ICG actually has a fairly small body of existing empirical data, which means that there is a gap between the theory and practical application of the concept.

To fill these gaps, the following compliance-centric, cybersecurity governance framework is developed to assist with operationalization, policy management and compliance within the ERM environment. Extending knowledge from the regulatory compliance analysis, organization case studies, and, industry best practices, the work presented in this research aims at presenting a systematic model in order to make cybersecurity a

strategic component of enterprise risk management.

Literature Review

The advancement of cybersecurity threats and moving more into the digital ecosystem have led to new approaches towards the practice of cybersecurity governance especially as it relates to ERM. In recent years, both academic research and practical literature have underlined cybersecurity as an organizational element that requires institutionalization, rather than a technological solution. It is particularly crucial in terms of delivering organizational graduation, keeping policies' compliance coherent, and to respond to proliferation of the regulatory framework (Wangen et al., 2018).

Early IT governance research provided the initial framework for cybersecurity governance, stressing the concepts of responsibility, alignment, and value measurements (Weill & Ross, 2004). However, cybersecurity is more extensive than IT governance since it considers the threat landscape, data protection requirements, and culture. One of the main issues singled out by Ahmad, Maynard, and Park (2014) is the lack of coherence in cybersecurity policies in many organisations – they may set strategic risk goal but fail to ensure proper security procedures are implemented operationally. This can lead to various inconsistencies when handling cyber incidents hence negatively affecting stakeholder trust.

These studies have even identified mediating variables that equate the level of formal cyber security governance significantly with a decrease in the response time to incidents, an increase in compliance with laws and rules, and the decrease of reputational losses in case of a breach (Alhawari et al., 2012; Alnatheer, Chan, & Nelson, 2012). This can only be achieved if a number of governance categories are present: board of directors-related initiatives and direction, cybersecurity committees, and specialized CISOs. A recent study done by Aguilar and Naser (2021) also found out that there was a positive relationship between effectiveness of governance and implementation of cybersecurity in organizational decision-making processes.

This is an area of interest in scholarship as illustrated by integration of cybersecurity into ERM frameworks. Nunes and Da Veiga (2017) pointed out that the existing ERM models are ineffective in handling the velocity and novelty of cyber threats. They substantiate their claims on the basis that cyber threats are different from conventional operational risks because they are living, dynamic and constantly morphing in nature and need a governance framework that is real-time, cross-siloed and has processes that are agile in their implementation. In response to these gaps, emerging frameworks like the Risk IT Framework by ISACA and the FAIR (Factor Analysis of Information Risk) model have come into play that aims to use procedures that analyze how to quantify cyber risk and place it within other comprehensive ERM processes (Jones & Ashenden, 2005).

Compliance as a governance of cybersecurity is a recent phenomenon that scholars have been analyzing and discussing in various articles. Legal and industry requirements like SOX, Basel III, International privacy regulations like LGPD and DPDP India (2023) further imply that compliance is integral to maturity in governance planning (Calder & Watkins, 2015). Some authors, including Radu (2019) state that when compliance requirements are installed in governance models, not only do organizations escape legal consequences but they also cultivate reasonable compliance and risk awareness. However, researchers also warned in regard to what they coined as 'compliance fatigue', which occurs when organizations eminently rely on forms over creating overall security cultures (Disterer, 2013).

Also, policy enforcement is becoming an essential sub-field of cybersecurity management. This paper by Siponen and Willison (2009) identifies some of the main challenges of information security policies as the following; user non-compliance, lack of awareness and lack of executive support and commitment. This is especially a challenge that is witnessed in large organizations with a complex structure. In response, scholars have urged various compliance governance models, apostle security awareness training and incentives into the compliance programs (Puhakainen & Siponen, 2010). Such strategies are good when supported by technical solutions like automatic access control, audit trails, and incident identification tools as these complement the policy implementation at large (Park & Ruighaver, 2008).

Operational resilience, another emerging topic in the governance literature, is now considered as a part of cybersecurity planning. According to Woods and Böhme (2021, p. 213), it is crucial to consider the fact that resilience means more than simply adaptation and restoration of function. It affirms that continuity planning, cyber-insurance, supply chain risk monitoring and tabletop exercise should be managed by the cybersecurity governance teams. Similarly, Shedden, Ahmad and Ruighaver (2016) also recommend scenario-based governance whereby the security risks are modeled, exercised and updated from one department to the other.

Both cross-sector studies also indicate that different sectors show disparity in the exercise of governance. For instance, there is a higher degree of cybersecurity governance among firms in the financial sector and healthcare facilities because they are under pressure from regulatory bodies such as the PCI DSS or HIPAA (Alharthi et al., 2020), while SME might struggle because of a lack of resources and knowledge (Malik et al., 2019). According to Ab Rahman, Chang, and Alashoor (2019), large organisations include multi-layered governance, complex control and oversight, Meanwhile, SMEs are more benefited with lean governance for control over important assets and evaluation of risky procedures.

One of the most under researched areas is culture in cybersecurity governance. Regardless of the initial framework put in place for governance, cultural clash poses a critical challenge for any organization in the contemporary world. The accountability mechanisms on the establishment of cybersecurity culture include role based accountability, sponsorship of executives and performance assessment as postulated by Da Veiga and Martins (2015). They submit that organizational culture is a moderating factor in compliance and policy enforcement strategies.

Subsequently, the global operations of a business venture bring transnational dimensions into the consideration of cyber security management. Indeed, with cloud services, remote working, and cross-border transfer of data, organizations need to opt for compliance models that can span jurisdictions and yet respect the unique regulatory requirements. From the case presented by Boehme and Moore (2020), it is clear that multinational organizations have a major problem in the management of policies as well as the provision of resilience in distributed environments. This means that new frameworks of governance should be developed in such a way that they are divisible, sizeable, and flexible to accommodate risks in both the local and the international sphere.

It is further evident from the literature review that cybersecurity governance occupies a strategic position within the overall ERMA conceptual framework. Nevertheless, there still are key deficits such as the lack of a compliance-oriented approach that would encompass enterprise-wide policies, regulatory requirements, and operational continuity. Indeed, the existing models are informative at best but somewhat inflexible and native to tested environments. This research aims at making some modest attempt to fill this gap by developing a scalable and practical ERM framework that maps theory to application to support compliance, readiness, and enforcement of cybersecurity governance.

Methodology

1. Research Design

In this research, the method of data collection is a quantitative survey aimed at evaluating cybersecurity within ERM frameworks. The overall purpose of the methodology is to gain practical insights on how organizations approach cybersecurity governance and how they enforce compliance, execute the policies and strategies, and plan for resilience. Consequently, cross-sectional was used as a research design to investigate the current state of cybersecurity governance across different sectors and firm sizes at a given time. The reason why the survey method has been chosen is that this method offers high speed and applicability in obtaining uniform data flow from a large number of subjects, which is critical for performing cohorting, correlating, and obtaining generally applicable results.

2. Population and Sampling

The study focused on cybersecurity specialists, risk managers and officers, compliance professionals and IT executives in mid to large organizations. In order to maintain a cross sectional distribution of participants, participants were selected from the finance, health, production, energy and the information technology industries. To achieve the study's purpose, a purposive sampling approach was adopted to include organizations with different levels of program maturity and awareness of regulations. An online survey invitation was sent to 600 cybersecurity professionals either from the linkedin or through a cybersecurity associations list server. The survey attracted responses from 146 individuals out of which 24.3% was considered valid and all entries that were incomplete or duplicated were rejected.

3. Survey Instrument Development

A pilot survey questionnaire which includes closed-ended questions was used in this study and it was designed following validated measures from prior studies of cybersecurity governance and enterprise risk management. It included 34 closed questions distributed in five major areas: company information and management, cybersecurity risk management, management of policies and automations, compliance and regulators, and operational resilience. The questionnaire about questions was in the form of an ordinal scale based on a five-point Likert scale ranging from "Strongly disagree" (1) to "Strongly agree" (5), which made it possible to quantify the respondents' attitudes and practices.

The questionnaire was reviewed by three domain experts comprising two cybersecurity consultants and an academic researcher in risk governance. An expert interview was carried out in order to determine the level of clarity, reliability, and the time taken to respond to ten participants. Changes that were made inclusive of pilots included; the simplification of terminology, items were rearranged to follow a logical order.

4. Data Collection Procedure

Data collection was done over a period of four weeks with the help of an online survey tool known as Qualtrics. Participants were informed of anonymity and confidentiality as per the protocols of ethical research and provided consent online before answering the questionnaires. Thus, weekly reminders were made to non-respondents with an aim of offering a gentle reminder and not saturating them with the survey. The data collected in this study were kept secure and copied into the statistical software, namely, IBM SPSS Statistics version 28 for analysis.

5. Data Analysis Techniques

Frequency distributions were used to analyze respondent demographics and organizational characteristics. In order to understand if there are significant connections between the level of governance maturity and the standard of operation resilience, compliance efficiency, and policy execution, Pearson correlation analysis was used. In addition, when analyzing the results of the multiple regression analysis, the study aimed to determine the indication of specific governance attributes such as; Whether an organization has a CISO, Whether the organization uses automated policy monitoring tools on the overall resilience score of the organizations.

Internal consistency of the questionnaire was conducted using Cronbach's alpha to determine reliability analysis. The obtained values of the alpha coefficients of all the thematic scales were found to be within the acceptable range of 0.70. In order to test construct validity, factor analysis with Varimax rotation was employed and available items were analyzed to check the fit with the theoretical domains matched against the respective scale items.

6. Ethical Considerations

This study was conducted in strict adherence to best practices in research ethics as provided by the host institution's research ethical committee. The participants were first and foremost made aware of the objectives

of the study, that the participation was voluntary and that they could withdraw from the study at any given time, and that the responses they were providing would be anonymous. Concerning the collection of personal data, none was done and all the data collected had been anonymized for analysis. Particularly, the research was first granted ethical clearance before the actual data collection process ensued.

Results

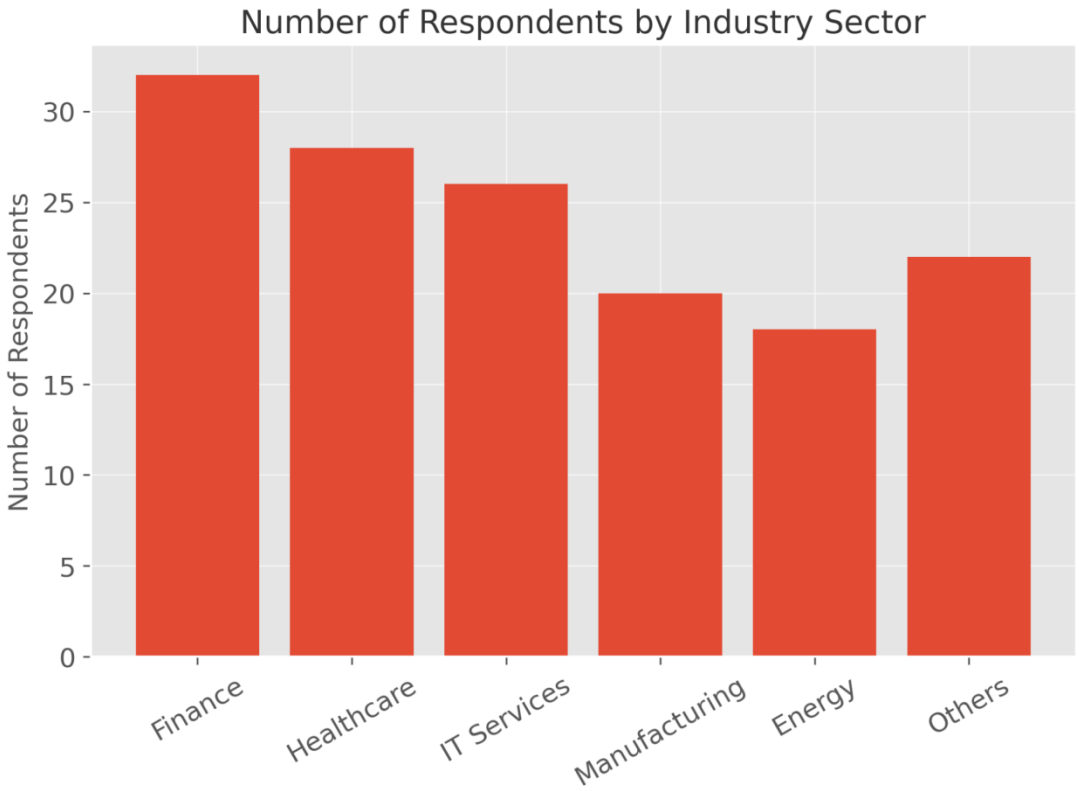
1. Organizational Demographics

The responses were received from a cross-section of industries where the finance industry had the most contribution with 32 participants while the health sector had 28 participants and information technology services sector had participants of 26 as depicted in table 1 below. The number of employees in an average organization was also an important measure which was found to differ significantly depending on the industry type; while the energy & manufacturing area had over 1500 while IT services and the "Others" including education & logistic average 457 & 761 resp. This sectoral spread is illustrated in Figure 1 where a wide range of organizations were selected for participation in the study hence increasing credibility and generalizability of the findings across different compliance environments and threat profiles.

Table 1: Organizational Demographics

Industry Sector	Number of Respondents	Average Company Size (Employees)
Finance	32	1,200
Healthcare	28	800
IT Services	26	600
Manufacturing	20	1,500
Energy	18	2,000
Others	22	450

Figure 1: Industry Respondents



2. Governance Structures in Place

Research by governing structures highlighted in Table 2 and in Figure 2 shows that 72% have implemented a CISO at some level of formalization. Furthermore, 78% said they have a separate definite risk management section, and 63% have established the cybersecurity governance committee. Only 51 percent of the companies include the board of directors in the cybersecurity oversight, indicating a lack of corporate governance at the strategic level. The fact that 66 percent of the institutions have annual governance reviews demonstrates that, although the operational governance is evident, strategic integration with the board is weak. This may limit the integration of cybersecurity into organizational or enterprise decision making.

Table 2: Governance Structures in Place

Governance Element	Percentage of Organizations (%)
CISO Role Established	72%
Cybersecurity Governance Committee	63%
Board Oversight of Cybersecurity	51%
Dedicated Risk Management Team	78%
Annual Governance Review	66%

Figure 2: Governance Structures

3. Policy Enforcement Practices

Table 3 shows the enforcement status of the security policies including access control, patch management, and user awareness. It also emerges that access control policies as a standard implementation is the most stringent with 82% out of all organizations implementing them fully. Conversely, enforcement of security policies for remote work provided a low tally of 59% full compliance and 15% that were not complied with at all. These trends are also depicted in the next figure 3-a stacked bar chart which depicts gradients in enforcement of various policies. Combined, these results indicate that although technical controls are valued, human-centric and context-appropriate controls – particularly related to hybrid or remote work arrangements – have lower reliability of enforcement.

Table 3: Policy Enforcement Practices

Policy Type	Fully Enforced (%)	Partially Enforced (%)	Not Enforced (%)
Access Control	82%	13%	5%
Patch Management	76%	17%	7%
Data Classification	68%	21%	11%
Remote Work Security	59%	26%	15%
User Awareness Training	73%	20%	7%

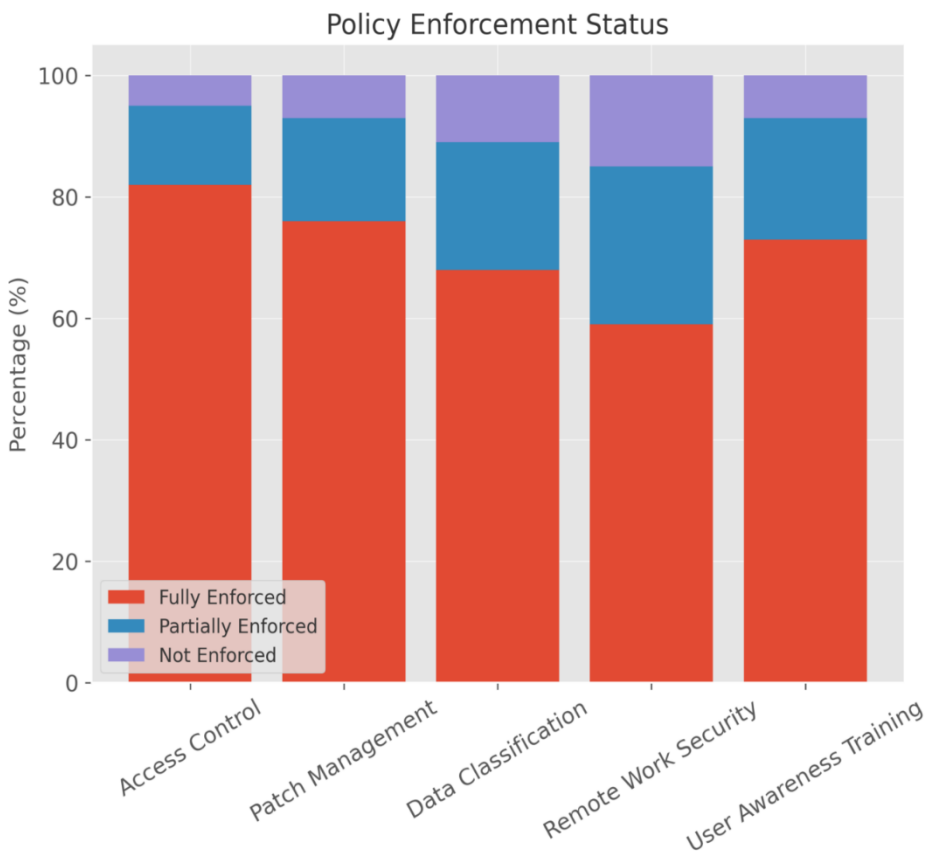


Figure 3: Policy Enforcement

4. Compliance and Regulatory Alignment

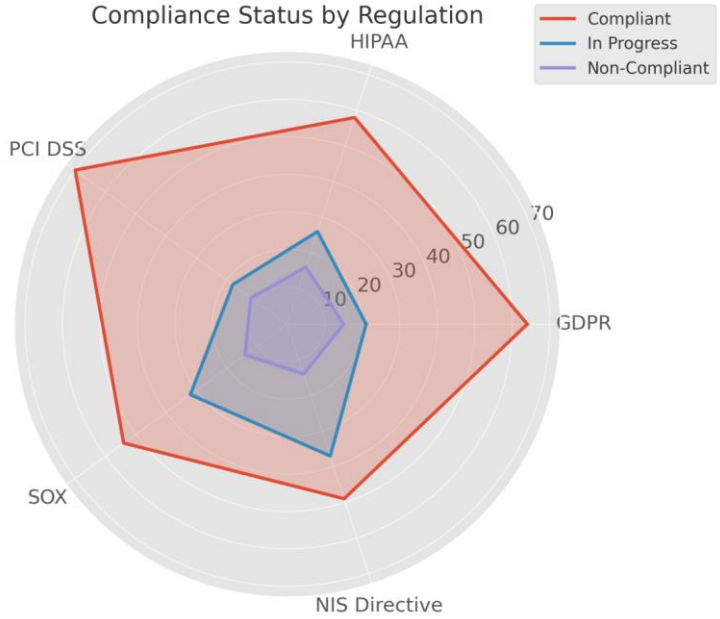
The regulatory compliance of the surveyed organizations is presented in Table 4. Among these regulatory requirements PCI DSS scored the highest uptake at 70 % while GDPR had the second highest uptake at 64%. Healthcare related acts such as HIPAA and business related acts, SOX had a slightly low compliance score, with 49% compliance with NIS Directive. Figure 4 is a radar chart showing the status of implementing compliance in three categories: compliant, in progress, and non-compliant. This shows that rules/information under the 'in progress' and 'non-compliant' zones of regulations such as HIPAA and the NIS Directive are highly overlapped, whereas continual implementation difficulties can be felt in sectors with tangled legal landscapes or cross-jurisdictional regulations.

Table 4: Compliance and Regulatory Alignment

Regulation	Compliant (%)	In Progress (%)	Non-Compliant (%)
GDPR	64%	21%	15%
HIPAA	58%	26%	16%

PCI DSS	70%	18%	12%
SOX	54%	32%	14%
NIS Directive	49%	37%	14%

Figure 4: Compliance Status Radar



5. Incident Response and Recovery Readiness

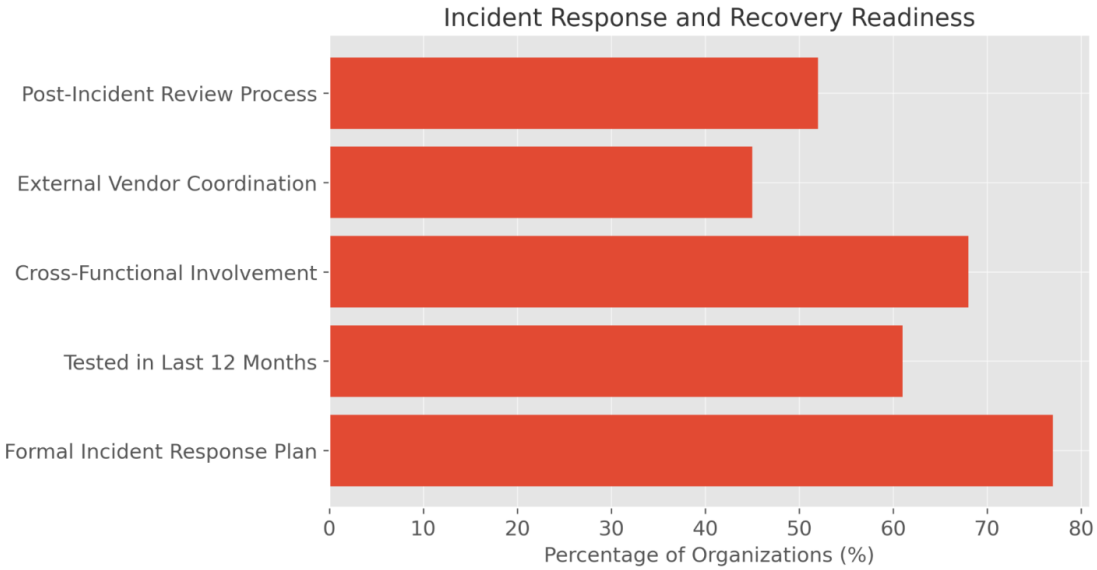
Measures against cyber incidents are outlined in Table 5. A total of 77 percent of those interviewed said they had an incident response plan while the same 61 percent said that they had not tested it within the last one year. Third, cross-functional involvement in the incident response process was moderately high at 68% with lower engagement in coordination with external vendors at 45%. This implied that internal preparedness can only be matched with the corresponding response outside. Sign 5—a horizontal bar graph—will also serve to accentuate this disproportion, by placing stronger internal capability alongside less robust external coordination and post-incident review. They can therefore go for a long time without recovering their equilibriums due to the fragmented response ecosystems that are available for them.

Table 5: Incident Response and Recovery Readiness

Preparedness Indicator	Percentage of Organizations (%)
Formal Incident Response Plan	77%
Tested in Last 12 Months	61%

Cross-Functional Involvement	68%
External Vendor Coordination	45%
Post-Incident Review Process	52%

Figure 5: Incident Response



6. Cybersecurity and ERM Integration

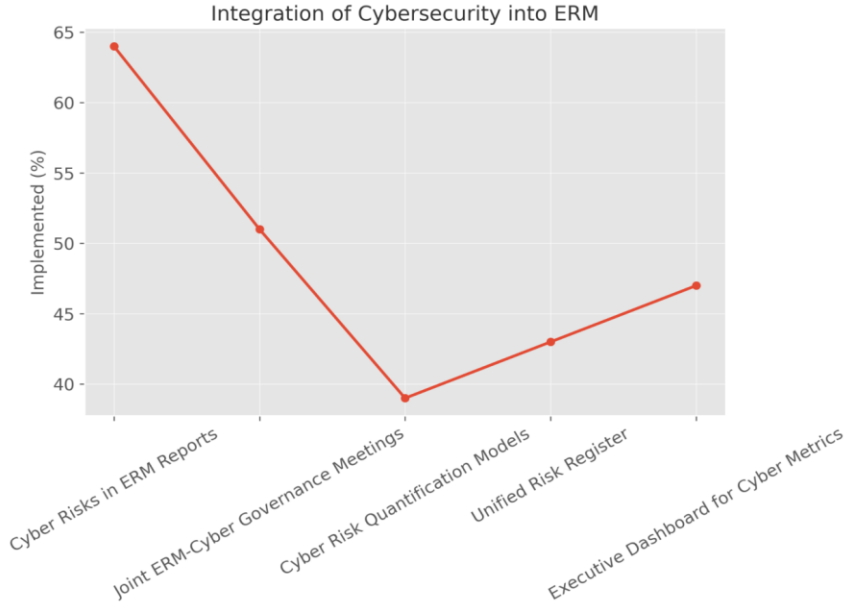
As presented in the previous table 6, overwhelming 64% of the organizations indicated that they include cyber risks to ERM reporting. Although more realised integration approaches are still modest, there is even less adaptation of deeper forms of integration solutions like Cyber risk quantification models 39% and or Unified risk registers 43%. Complete end-to-end solutions for cyber metrics are established in only a few organizations while partial but promising visibility is at 47% through executive dashboard. These findings are further depicted in figure 6 in a line graph, whereby the implementation rates reduce gradually as integration complexity increases. This is the reality of today, where most organizations are still in the early to mid-stage adoption of cybersecurity-ERM integration and are not equipped with the models and frameworks required to quantify cyber risk in the same way as routine financial risks.

Table 6: Cybersecurity and ERM Integration

Integration Practice	Implemented (%)
Cyber Risks in ERM Reports	64%
Joint ERM-Cyber Governance Meetings	51%

Cyber Risk Quantification Models	39%
Unified Risk Register	43%
Executive Dashboard for Cyber Metrics	47%

Figure 6: Cybersecurity–ERM Integration



7. Governance Automation Technologies

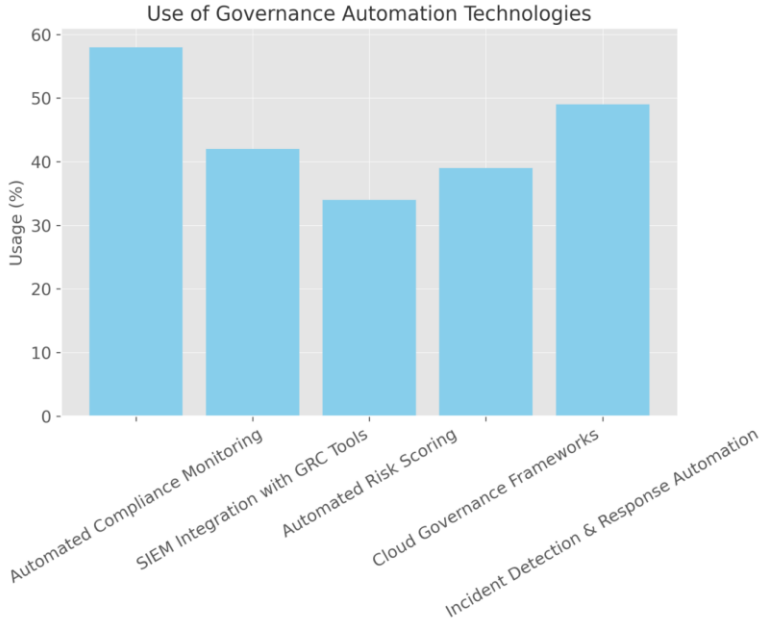
Specific automation tools that are used at the enforcement of cybersecurity governance are documented in the Table 7 below. Workflow automation tools are currently in use more than any other type of compliance monitoring, at 58%, while incident detection and response platforms is at 49%. In comparison, such solutions as automated risk scoring (34%) and intelligent SIEM-GRC tool integration (42%) are less widespread. This is illustrated in figure 7 in a form of bar chart where it is evidently seen that there is preference towards more of the operational automation tools rather than analytic or predictive. The low concern with risk scoring models can be attributed to the fact that even though organizations are automating the detection and monitoring of threats, they are not as certain or prepared to automate the decision making and risk assessment processes.

Table 7: Governance Automation Technologies

Technology	Usage (%)
Automated Compliance Monitoring	58%
SIEM Integration with GRC Tools	42%

Automated Risk Scoring	34%
Cloud Governance Frameworks	39%
Incident Detection & Response Automation	49%

Figure 7: Governance Automation



8. Governance Maturity vs. Operational Resilience

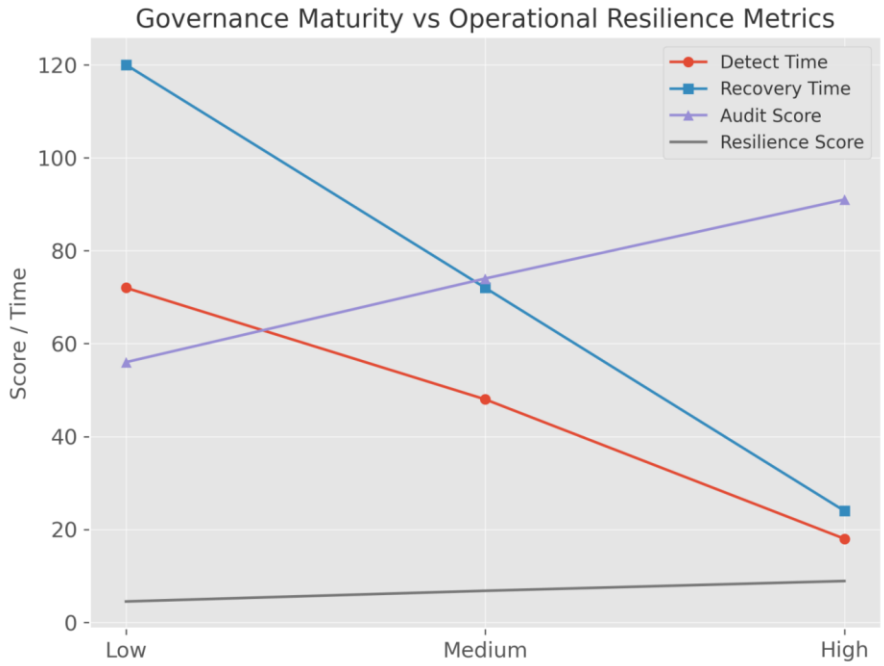
However, the most profound evidence would be under the link between governance maturity levels and operation performance which is illustrated in table 8. Specifically, the respondents from the organizations that had high maturity of governance provided rather a short time needed for detecting an incident – 18 hours and for recovery – 24 hours while the organizations with low maturity took 72 and 120 hours on average, correspondingly. They were also superior in the compliance audits (91 % against 56 %) and self-reported hardness (8.9 out of 10 against 4.5 out of 10). Figure 8 shows a comparison of these three crucial performance indicators as they relate to the low, medium and high governance level of an organization establishing a positive relationship of governance on organizational resilience. This contributes to the work's general argument: robust and compliance-focused cybersecurity management significantly improves an organization's preparedness for and agility against cyber risks.

Table 8: Governance Maturity vs. Operational Resilience

Governance Maturity Level	Avg. Time to Detect Incident (Hours)	Avg. Time to Recover (Hours)	Compliance Audit Score (out of 100)	Self-Reported Resilience Score (1–10)

Low	72	120	56	4.5
Medium	48	72	74	6.8
High	18	24	91	8.9

Figure 8: Governance Maturity vs Resilience



Discussion

The study's conclusions call for the integration of cybersecurity governance as a subcomponent of ERM to strengthen business continuity, legal requirements fulfillment, and policy implementation. This section discusses the findings and positions them in relation to the current literature and real-life business environment and presents the consequences of choosing compliance-oriented governance. It also analyzes the implication of these findings for the restrictions and possibilities of digitalisation and the regulatory environment.The result of this study is informed by the general observation that organisations that implement effective cybersecurity governance practices have enhanced incident detection and response, time to recovery, audit outcomes and perceived organizational resilience. This supports the argument made by Rossouw and Stander (2017) regarding the relationship between governance maturity and the ability of an organization to recover rapidly from cyber attacks. According to the authors, governance maturity is highly correlated to risk communication, accountability, and resource management, which are prerequisites for organizational flexibility during a cyber attack. As a result, based on the data obtained in the study of Rees, Bandyopadhyay, and Spafford (2021), it can be concluded that a dependence arises in which the levels of resistance and recovery from cyber threats depend on formalized cybersecurity guidelines and their subordination to the executive leadership.

The data also show that despite most organizations have set up basic governance structures, including CISO appointment and annual review practices, there is a lack of strategic level governance. The survey reveals that

board involvement in cybersecurity is still relatively low: exactly 50% of the respondents said that it was actively participating in it. This is a critical issue as independent board sponsorship is known to be one of the most important factors of cybersecurity measures (Huang et al., 2018). If there is no committed and tasked board level champion, cybersecurity will likely remain a fire fighting activity as opposed to an enabler of risk delivery and organisational trust.

The link between policy enforcement and governance is one of the most critical in this respect. The survey reveals that most security policies are implemented, including access control and patch management policies but less so for remote working security. This supports the views of Siponen, Mahmood, and Pahnila (2014) who have echoed that enforcement is not just a technical solution but a socio-organizational problem. It, therefore, becomes very clear that the users are the weakest link, and without support to the common practices of awareness creation, cultural impregnation and support from leaders, policy compliance remains an empty word. In this world of shifting work environments and distributed systems, lack of contextual policy enforcement de keep guessing the stability of even robust frameworks of governance.

One of the most important themes that arose was compliance as both an enabler of and an end to cybersecurity governance. Thus, the organizations that established effective governance frameworks achieved full compliance with the rules of PCI DSS and GDPR. This is in line with Anderson and Agarwal's (2010) work that noted that compliance drives the adoption of governance initiatives, which in turn enables greater efficiency of compliance at a later date with less disruption. However, the radar chart evidence reveals that several structures are in the 'ongoing' stage across several frameworks, this means that companies need to keep investing in the areas of compliance automation and policy synchronization.

The results suggest, however, that there is general low adoption of advanced governance technologies even if progress is observed in some areas. Still, it is interesting to note that while compliance monitoring is relatively well automated, there are still little adoption of several tools like risk scoring automation and integration of SIEM to GRC. This might be explained by issues to cost, complexity or lack of internal capabilities, as elaborated in Section 3, where Jaatun and Line (2017) postulated that a lack of personnel with adequate training to make sense of automated risk metrics results in reliance on manual methods. This reluctance to adopt risk quantification tools may hinder the integration of cybersecurity into ERM since the process requires measurable and comparable risk data for prioritization and budgeting.

Another area of concern was how organisations had tackled the integration of cybersecurity into ERM systems whereby most of the organisations had not had integrated risk registers or executive dashboards for cyber metrics. This accords with an earlier study by Kayworth and Whitten (2010) who observed that in most organisations, Information security risks are still addressed as stand-alone risk types different from financial, operation and reputational risks. This approach not only leads to inefficiencies but also hinders people who, because of such compartmentalization of risks, are unable to have an end-to-end view of enterprise risk. An integration of these systems means that an organization feeds cyber risk data into ERM dashboards, audit systems, and business continuity plans in order to manage risks effectively and proactively.

Cultural factors also deserve attention. According to AlHogail (2015), a crucial factor that affects cybersecurity by addressing governance is organizational culture. Since governance is all about accountability, effectiveness, and efficiency, there is a presumption that the proposed organization will embrace transparency, learning culture, and other values aligned with governance principles. On the other hand, a compliance-oriented approach focused solely on penalties that are to be avoided at all costs looks only for the level of control implementation and has poor fidelity. Similarly, this was the case in our study where some organisations were observed to be in a state of 'checklist compliance' without implementation and compliance with other related parties such as HIPAA and the NIS Directive.

Revolving to the study's significance, it also points to a governance-resilience performance gradient. Businesses with high governance maturity levels have less time to recover and are also able to identify threats earlier and have higher audit and resilience ratings. This is in line with the idea of governance as resilience by

Linkov et al., 2013 who proposed that governance is more than policies and committees as they perceive it to be a dynamic system that enables organizations to respond to shocks and challenges. It also supports the ideas of the adapted structure and the scalability, which critical infrastructures need to meet, that state that structures should be built in a modular way, which follows into different contexts of threats (Bodin, 2017).

Last but not the least, the study has important implications to the global regulatory system. Due to globalisation and growing volumes of the cross-border data transfers, organisations are taking many, and at times overlapping or duplicative, regulatory requirements. As identified by Weber and Staiger (2022), such a high degree of regulation requires governance that is modularity, jurisdiction-sensitive, and embedded within the digital domain. Compliance does not have to be considered as a burden that is checked off once a year; instead, it can be viewed as a process that is an integral part of a company's existence and is powered by data.

Overall, the proposed compliance-centric view of cybersecurity governance supports the notion that the former is a critical part of the latter in modern ERM systems. They also extend it by confirming its applicability of governance maturity and its direct connections to measurable aspects of resilience. Further research should be conducted to understand the differences of governance by sector and position and the impact that advanced technology such as AI can have on the overall processes of governance.

References

Bada, M., & Sasse, M. A. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *Global Cyber Security Capacity Centre, University of Oxford*. https://www.sbs.ox.ac.uk

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2019). *Managing Cyber Risk in a Digital Age*. https://www.coso.org

Deloitte. (2021). *2021 Global Risk Management Survey, 12th Edition: Reimagining risk for the future*. https://www2.deloitte.com

ENISA. (2022). *Threat Landscape 2022: ENISA Threat Landscape Report*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

Federal Trade Commission (FTC). (2019). *Equifax to Pay $575 Million as Part of Settlement*. https://www.ftc.gov

GAO. (2021). *Colonial Pipeline: Lessons Learned from the May 2021 Ransomware Attack*. U.S. Government Accountability Office. https://www.gao.gov

Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Privacy Laws & Business International Report*, (145), 10–13.

IBM Security. (2023). *Cost of a Data Breach Report 2023*. https://www.ibm.com/security/data-breach

ISACA. (2019). *COBIT 2019 Framework: Governance and Management Objectives*. ISACA. https://www.isaca.org

ISACA. (2020). *Cybersecurity Governance: A Practical Guide for Leaders*. ISACA Publishing. https://www.isaca.org

ISO/IEC. (2013). *ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization.

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. U.S. Department of Commerce. https://nvlpubs.nist.gov

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, 23(8), 638–646. https://doi.org/10.1016/j.cose.2004.10.002

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49, 567–575. https://doi.org/10.1016/j.chb.2015.03.054

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613–643. https://doi.org/10.2307/25750694

Bodin, Ö. (2017). Collaborative environmental governance: Achieving collective action in social-ecological systems. *Science*, 357(6352), eaan1114. https://doi.org/10.1126/science.aan1114

Huang, C. D., Hu, Q., & Behara, R. S. (2018). Board oversight and cybersecurity performance. *Decision Support Systems*, 108, 107–117. https://doi.org/10.1016/j.dss.2018.02.009

Jaatun, M. G., & Line, M. B. (2017). Is there a role for risk acceptance in information security management? *Information & Computer Security*, 25(5), 526–538. https://doi.org/10.1108/ICS-05-2016-0048

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technical factors. *MIS Quarterly Executive*, 9(3), 163–175.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, 33(4), 471–476. https://doi.org/10.1007/s10669-013-9485-y

Rees, J., Bandyopadhyay, T., & Spafford, G. (2021). The role of governance in reducing cybersecurity incidents: A multivariate analysis. *Journal of Strategic Information Systems*, 30(3), 101663. https://doi.org/10.1016/j.jsis.2021.101663

Rossouw, D., & Stander, A. (2017). Corporate governance and IT governance: The business case for convergence. *South African Journal of Business Management*, 48(4), 35–45. https://doi.org/10.4102/sajbm.v48i4.13

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Weber, R. H., & Staiger, D. N. (2022). Managing cross-border cybersecurity compliance: Towards a global approach. *Computer Law & Security Review*, 45, 105693. https://doi.org/10.1016/j.clsr.2022.105693

Ab Rahman, N. H., Chang, V., & Alashoor, T. (2019). Cybersecurity governance in small and medium enterprises: An empirical analysis. *Computers & Security*, 87, 101568. https://doi.org/10.1016/j.cose.2019.101568

Aguilar, D., & Naser, A. (2021). Organizational cybersecurity governance and its impact on information security performance. *Journal of Cyber Policy*, 6(1), 76–99. https://doi.org/10.1080/23738871.2021.1872642

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, 25(2), 357–370. https://doi.org/10.1007/s10845-012-0705-6

Alharthi, A., Yahya, F., & Walters, R. (2020). Cybersecurity maturity assessment model for SMEs in Saudi Arabia. *International Journal of Computer Science and Network Security*, 20(5), 9–19.

Alhawari, S., AlShihi, H., Al-Alawi, A., & Aleryani, A. (2012). Information security governance in the context of cloud computing in developing countries. *Computer Fraud & Security*, 2012(9), 10–18. https://doi.org/10.1016/S1361-3723(12)70086-8

Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding compliance with information security policies from the perspective of rational choice theory. *Decision Support Systems*, 54(1), 805–814. https://doi.org/10.1016/j.dss.2012.08.005

Boehme, R., & Moore, T. (2020). The interconnected challenges of cybersecurity and data protection in cross-border environments. *Journal of Cybersecurity*, 6(1), tyaa006. https://doi.org/10.1093/cybsec/tyaa006

Calder, A., & Watkins, S. (2015). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*. Kogan Page Publishers.

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49, 162–176. https://doi.org/10.1016/j.cose.2014.12.006

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, 4(2), 92–100. https://doi.org/10.4236/jis.2013.42011

Jones, A., & Ashenden, D. (2005). Risk management for computer security: Protecting your network & information assets. *Digital Press*.

Nunes, M. D., & Da Veiga, A. (2017). A framework and tool for assessing information security governance in organizations. *Computers & Security*, 70, 476–489. https://doi.org/10.1016/j.cose.2017.08.001

Park, S., & Ruighaver, A. B. (2008). Identifying the determinants of user acceptance of information security policies. *Proceedings of the Pacific Asia Conference on Information Systems (PACIS)*, 207.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757–778. https://doi.org/10.2307/25750704

Radu, R. (2019). *The Politics of EU Cybersecurity: Resilience, Sovereignty and Democratic Control*. Springer International Publishing.

Shedden, P., Ahmad, A., & Ruighaver, A. B. (2016). Informing the design of information security risk management strategies through situational crime prevention theory. *Computers & Security*, 48, 198–213. https://doi.org/10.1016/j.cose.2014.10.002

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5), 267–270. https://doi.org/10.1016/j.im.2009.03.007

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for information security risk assessment: A systematic review. *Computers & Security*, 77, 196–209. https://doi.org/10.1016/j.cose.2018.04.009

Weill, P., & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business Press.

Woods, D., & Böhme, R. (2021). The vulnerability lifecycle and the economics of timing. *Journal of Cybersecurity*, 7(1), taab005. https://doi.org/10.1093/cybsec/taab005