Int. j. adv. multidisc. res. stud. 2024; 4(6):2127-2139

Received: 11-11-2024
Accepted: 21-12-2024

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Enhancing Cybersecurity Governance in Financial Institutions: A Quantitative Study on Control Deficiencies and Regulatory Compliance

[1] Adetola Adewale Akinsulire, [2] Tochi Chimaobi Ohakawa
[1] Mixta Africa Group Lagos, Nigeria
[2] Independent Researcher, USA

DOI: https://doi.org/10.62225/2583049X.2024.4.6.4264
Corresponding Author: **Adetola Adewale Akinsulire**

Abstract
The increasing frequency and sophistication of cyber threats in the financial sector have underscored the critical need for robust cybersecurity governance. This study explores the control deficiencies in cybersecurity governance within financial institutions and assesses their impact on regulatory compliance. By adopting a quantitative approach, the research identifies common gaps in cybersecurity controls, measures their correlation with regulatory adherence, and analyzes the consequences of non-compliance. Through surveys, audits, and case studies of financial institutions, the study examines the role of IT governance frameworks, such as COBIT, NIST, and ISO 27001, in addressing cybersecurity risks and ensuring regulatory compliance. The findings reveal that many financial institutions struggle with control deficiencies, particularly in areas like incident response, vulnerability management, and third-party risk oversight. These deficiencies often lead to regulatory non-compliance, exposing institutions to significant financial, legal, and reputational risks. Additionally, the study highlights how an ineffective alignment between IT governance and business objectives exacerbates these challenges. The research further explores the regulatory landscape, including frameworks like GDPR, GLBA, and PCI DSS, which require financial institutions to maintain robust cybersecurity measures and regular compliance audits. In response, this proposes several strategies for enhancing cybersecurity governance, including strengthening IT governance frameworks, improving control measures, and fostering a culture of continuous cybersecurity awareness and compliance. The review emphasizes the need for institutions to invest in resources, tools, and training to address control gaps and ensure effective risk management. Overall, this research contributes to a deeper understanding of how control deficiencies impact cybersecurity governance and regulatory compliance, offering actionable insights for financial institutions to enhance their resilience against evolving cyber threats.
Enhancing in: A on Control.

Keywords: Cybersecurity, Governance, Financial Institutions, Quantitative Study, Deficiencies and Regulatory Compliance

1. Introduction

Cybersecurity governance has become a critical aspect of operational management within financial institutions, given the increasing prevalence and complexity of cyber threats (Uddin *et al*., 2020) [63]. Cybersecurity governance involves the strategic alignment of an organization's cybersecurity policies, procedures, and resources with its overall business objectives. For financial institutions, this alignment is not just a best practice; it is a regulatory necessity to protect sensitive financial data, maintain customer trust, and ensure long-term operational stability (Aldboush and Ferdous, 2023) [6]. In recent years, financial institutions have faced growing pressure to adopt more comprehensive cybersecurity frameworks due to the rising number and sophistication of cyberattacks, which can lead to significant financial and reputational damage. Consequently, understanding and addressing deficiencies in cybersecurity governance are essential for safeguarding these institutions against emerging risks (Yusif and Hafeez-Baig, 2021) [70].

Cybersecurity governance refers to the process by which organizations direct and control their cybersecurity efforts to ensure they meet both business objectives and regulatory requirements (Bongiovanni *et al*., 2022; Boeding *et al*., 2022) [18, 16]. Within financial institutions, cybersecurity governance is paramount due to the nature of the industry, where even a minor breach or

lapse in control can have dire consequences (Wang *et al*., 2024) [68]. Effective cybersecurity governance establishes clear responsibilities and accountability, integrates risk management practices, and supports compliance with relevant laws and regulations. Given the critical role financial institutions play in the economy, they must adhere to strict governance models to protect not just their assets, but also the financial stability of their clients and broader economic systems.A comprehensive cybersecurity governance framework is built upon several key components: IT governance, risk management, compliance, and internal controls (Melaku, 2023) [43]. IT governance ensures that cybersecurity policies align with the institution's strategic goals, while risk management identifies, assesses, and mitigates potential cyber risks that could impact operations. Compliance ensures adherence to legal and regulatory standards (such as GDPR, GLBA, or PCI DSS), while internal controls focus on monitoring and protecting systems from unauthorized access or cyberattacks (Aslam *et al*., 2022) [12]. The synergy of these components ensures that the institution's cybersecurity efforts are coordinated, effective, and responsive to emerging threats.

In recent years, financial institutions have witnessed a sharp rise in cyber threats, ranging from ransomware attacks and data breaches to more sophisticated tactics such as advanced persistent threats (APTs). The threat landscape is evolving at an alarming rate, with cybercriminals employing more complex and targeted methods to breach systems and exfiltrate sensitive financial data (Perwej *et al*., 2021) [53]. These attacks are not only more frequent but are also increasingly sophisticated, involving advanced malware and phishing techniques designed to exploit vulnerabilities in outdated systems. Financial institutions, with their vast amounts of sensitive data and monetary assets, are prime targets for such malicious activities. As digital transformation accelerates across the sector, institutions are becoming more interconnected, which expands their attack surface and exposes them to even greater risks.The consequences of cybersecurity breaches in financial institutions extend beyond financial losses to include long-term damage to reputation and customer trust (Paul *et al*., 2023) [51]. A successful cyberattack can lead to significant financial loss through fraud, fines, and operational disruptions. Furthermore, the reputational damage can be irreversible, as customers may lose confidence in the institution's ability to protect their sensitive information. This loss of trust can result in customer attrition, a decline in market share, and a tarnished brand image. The regulatory repercussions of a breach, including fines and penalties for non-compliance with established cybersecurity laws, can exacerbate these effects (Marotta and Madnick, 2021) [42]. Financial institutions must therefore prioritize cybersecurity to safeguard their stability, ensure regulatory compliance, and maintain the trust of their customers and stakeholders.

This review aims to analyze the state of cybersecurity governance in financial institutions, with a particular focus on identifying and addressing control deficiencies that may expose organizations to undue risk. Specifically, it will explore the various gaps in cybersecurity governance that can hinder financial institutions from effectively mitigating cyber threats and adhering to regulatory requirements. Understanding these control deficiencies is crucial, as it allows institutions to implement corrective actions and enhance their overall cybersecurity posture.The review will delve into the common control deficiencies that financial institutions face, such as inadequate incident response procedures, outdated security systems, and a lack of comprehensive employee training. These deficiencies often stem from resource constraints, a misalignment between IT governance and business objectives, or a failure to keep pace with evolving cybersecurity threats. By identifying these gaps, the review will highlight key areas that need immediate attention for improved cybersecurity governance.

Another central focus of this study is the interplay between control deficiencies, regulatory compliance, and cybersecurity risks. Inadequate cybersecurity governance can lead to failure in meeting regulatory requirements, exposing institutions to legal risks and penalties. Moreover, control deficiencies amplify cybersecurity risks, making financial institutions more vulnerable to attacks. This review will investigate how these factors are interrelated and the impact they have on the institution's overall security posture.A quantitative approach will be employed to measure the extent of governance gaps in financial institutions. This will involve the collection of data through surveys, audits, and case studies to assess the effectiveness of existing cybersecurity controls. The review will utilize statistical methods to quantify the relationship between governance deficiencies and cybersecurity risks, enabling a data-driven understanding of how these gaps can be addressed. By doing so, the review will provide actionable insights for financial institutions seeking to enhance their cybersecurity governance practices and achieve better regulatory compliance. As the frequency and sophistication of cyber threats continue to grow, effective cybersecurity governance becomes increasingly vital for financial institutions (Darem *et al*., 2023) [21]. By identifying and addressing control deficiencies, financial institutions can improve their resilience to cyber risks, safeguard their reputation, and ensure regulatory compliance. This review will contribute to the body of knowledge in the field of cybersecurity governance and offer practical recommendations for financial institutions looking to enhance their security frameworks.

2. Methodology

The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology will be employed to systematically review the relationship between cybersecurity governance, control deficiencies, and regulatory compliance in financial institutions. This methodology ensures a transparent, rigorous, and reproducible process for synthesizing quantitative data derived from relevant studies. The review will aim to evaluate how cybersecurity governance practices in financial institutions influence control deficiencies and compliance with regulatory frameworks.

Inclusion criteria for studies in this review will focus on research involving financial institutions such as banks, insurance firms, and investment companies. The studies must assess the impact of cybersecurity governance mechanisms—such as risk management practices, security frameworks, or regulatory compliance measures—on the occurrence of control deficiencies. The studies should provide quantifiable data on control deficiencies, including vulnerabilities, breaches, or incidents of non-compliance with regulatory frameworks, and their associated outcomes.

Only quantitative study designs, such as surveys, audits, or statistical analyses, will be included in this review.

A comprehensive search will be conducted across various databases, including Google Scholar, Scopus, IEEE Xplore, PubMed, and SpringerLink. Additionally, grey literature, such as reports from cybersecurity advisory firms and regulatory bodies, will be reviewed for relevant data. A search strategy will involve a combination of relevant keywords like "Cybersecurity Governance," "Control Deficiencies," "Regulatory Compliance," "Financial Institutions," and "Cybersecurity Risk Management," using Boolean operators to refine results. For instance, search terms will be combined as follows: ("Cybersecurity Governance" AND "Control Deficiencies" AND "Financial Institutions") OR ("Regulatory Compliance" AND "Cybersecurity Risks" AND "Banks").

The study selection process will involve screening titles and abstracts of identified articles to assess their relevance. Full-text reviews will be conducted for studies meeting the inclusion criteria, and data will be extracted from each study, including the study design, sample size, cybersecurity governance practices, identified control deficiencies, and regulatory compliance outcomes. The quality of each study will be assessed using established quality assessment tools such as the Critical Appraisal Skills Programme (CASP) for quantitative studies.

Data extraction will focus on essential details, including the authors, year of publication, country or region of the financial institution, sample size, measurement of cybersecurity governance, and reported outcomes related to control deficiencies and regulatory compliance. Key variables such as the implementation of risk management strategies, specific cybersecurity frameworks, and the presence of compliance measures will be included. Moreover, information regarding the frequency of breaches, vulnerabilities, regulatory fines, and penalties will be collected.

Data synthesis will aggregate the findings to evaluate the impact of cybersecurity governance on reducing control deficiencies and ensuring regulatory compliance. If sufficient homogeneity is found across studies, a meta-analysis will be conducted. Otherwise, a narrative synthesis will be provided. Subgroup analyses may be performed to explore differences based on the type of financial institution or geographical region.

The risk of bias in included studies will be assessed using the Cochrane Risk of Bias tool or relevant tools for quantitative research. Sources of bias such as selection bias, reporting bias, and measurement bias will be evaluated. This review will also focus on identifying the effectiveness of cybersecurity governance frameworks in reducing control deficiencies and promoting regulatory compliance.

The primary outcomes for analysis will be the relationship between cybersecurity governance practices and the frequency or severity of control deficiencies, as well as the impact of regulatory compliance on reducing security incidents and penalties. The study flow will be illustrated using a PRISMA diagram, showing the number of records identified, screened, and included, as well as the reasons for exclusions.

The discussion will provide an interpretation of the findings, considering the impact of cybersecurity governance on control deficiencies and regulatory compliance within financial institutions. Limitations of the included studies, such as variations in measurement approaches or biases, will be addressed. Implications for cybersecurity governance strategies in financial institutions will be discussed, with recommendations for improving regulatory compliance and reducing control deficiencies. This study will offer valuable insights into the role of cybersecurity governance in minimizing control deficiencies and enhancing regulatory compliance in financial institutions. The PRISMA methodology will ensure a transparent, systematic, and reproducible approach to synthesizing quantitative data, providing a comprehensive understanding of the topic.

2.1 Theoretical Framework

The theoretical framework for enhancing cybersecurity governance in financial institutions revolves around several key concepts. IT governance and cybersecurity frameworks, cybersecurity risk management, and regulatory compliance. Together, these frameworks provide the foundation for understanding how financial institutions can develop robust cybersecurity strategies, mitigate risks, and ensure regulatory adherence.

IT governance is the process by which organizations direct and control their IT resources to ensure alignment with business objectives. In the context of cybersecurity, IT governance plays a critical role in setting policies, procedures, and controls to protect against cyber threats (Savaş and Karataş, 2022) [56]. Several frameworks are widely adopted to guide IT governance in financial institutions; COBIT (Control Objectives for Information and Related Technologies)is a comprehensive framework that provides guidelines for IT governance, focusing on aligning IT with business goals, ensuring effective risk management, and improving operational efficiency. COBIT defines governance and management objectives that financial institutions must meet to ensure proper cybersecurity practices, including setting up appropriate risk and security controls (Adrian and Wang, 2023) [3]. It enables organizations to assess the maturity of their IT and cybersecurity controls.ITIL (Information Technology Infrastructure Library)is a set of practices for IT service management (ITSM) that emphasizes aligning IT services with the needs of the business. In cybersecurity governance, ITIL provides a structured approach to incident management, change management, and security management (Shinde and Kulkarni, 2021) [57]. It helps financial institutions ensure their IT infrastructure is resilient to cyberattacks and disruptions.ISO 27001 is a global standard for information security management systems (ISMS). It outlines best practices for managing sensitive company information, ensuring its confidentiality, integrity, and availability. This framework is particularly relevant to financial institutions because it focuses on risk management, continuous improvement, and the establishment of a formal ISMS that addresses cybersecurity threats.NIST (National Institute of Standards and Technology)provides a cybersecurity framework widely used in the United States and globally. NIST's Cybersecurity Framework (CSF) is designed to help organizations identify, protect against, detect, respond to, and recover from cyber incidents. NIST emphasizes a risk-based approach, which is critical for financial institutions in maintaining an adaptive and resilient cybersecurity posture (Thomas and Sule, 2023) [62].

Effective IT governance ensures that cybersecurity policies are not only compliant with regulations but also strategically aligned with the broader objectives of the financial

institution. By aligning cybersecurity with business goals, financial institutions can balance risk management, innovation, and operational efficiency (Abrahams *et al*., 2023) [2]. IT governance frameworks, such as COBIT and NIST, help establish clear policies, ensuring that the financial institution's resources are deployed efficiently to protect sensitive data, maintain business continuity, and support long-term growth. These frameworks guide organizations in integrating cybersecurity efforts into overall business processes, ensuring that cybersecurity is an enabler of business objectives rather than a hindrance.

Cybersecurity risk management is essential for identifying, assessing, and mitigating risks associated with cyber threats (Bokan and Santos, 2021) [17]. In financial institutions, the risks are multifaceted, involving both external and internal threats. Key cybersecurity risks include; Financial institutions hold vast amounts of sensitive data, making them prime targets for data breaches (Paul *et al*., 2023) [51]. These breaches can result from both external hackers and internal actors who gain unauthorized access to confidential customer or financial information.Ransomware attacks, where malicious actors encrypt critical data and demand payment for its release, have become a significant threat to financial institutions. These attacks can disrupt operations, damage reputations, and lead to significant financial losses.Insider threats, whether from disgruntled employees or contractors, pose a significant risk to the integrity and security of financial institutions. These threats are often difficult to detect and can involve the unauthorized access, theft, or manipulation of sensitive data.Cybercriminals often employ phishing and social engineering techniques to deceive employees into divulging sensitive information. These tactics can lead to unauthorized system access and financial fraud.

Cybersecurity risk management is intrinsically linked to the overall resilience of financial institutions. A proactive risk management strategy helps institutions identify potential vulnerabilities, assess the severity of threats, and implement controls to mitigate risks before they can manifest. Resilient institutions are those that can withstand and recover from cyberattacks, minimizing financial and operational disruption. By incorporating cybersecurity risk management practices, such as threat monitoring, incident response plans, and business continuity planning, financial institutions can enhance their capacity to respond to and recover from cyber incidents (Shukla *et al*., 2022) [58]. Effective risk management enables financial institutions to reduce the impact of cyber threats, maintain customer trust, and protect their financial stability.

Cybersecurity governance in financial institutions is significantly shaped by regulatory frameworks designed to protect sensitive financial data and ensure secure operations. Key regulatory standards include; GDPR (General Data Protection Regulation)is a regulation in the European Union that mandates strict data protection measures for organizations handling personal data. For financial institutions, GDPR compliance means adopting robust cybersecurity measures to protect customer data from unauthorized access and breaches, with severe penalties for non-compliance.GLBA (Gramm-Leach-Bliley Act)imposes requirements on U.S. financial institutions to safeguard consumer information. It mandates the implementation of effective cybersecurity controls to protect financial data and requires regular risk assessments and audits.PCI DSS (Payment Card Industry Data Security Standard)is a set of standards designed to protect credit card information. Financial institutions that handle payment card transactions must comply with PCI DSS to ensure the security of payment systems and prevent data breaches (Bhutta *et al*., 2022) [15]. FFIEC (Federal Financial Institutions Examination Council) provides guidelines for financial institutions in the U.S. to manage cybersecurity risks. The FFIEC's cybersecurity assessment tool helps institutions assess their cybersecurity maturity and implement necessary improvements.

Regulatory frameworks such as GDPR, GLBA, PCI DSS, and FFIEC play a vital role in shaping the cybersecurity governance practices of financial institutions. These regulations mandate the implementation of specific cybersecurity measures, such as data encryption, access controls, incident response plans, and regular audits. Compliance with these regulations helps institutions align their cybersecurity governance with industry standards, protecting sensitive customer data and maintaining trust (Haber *et al*., 2022) [30]. Additionally, these regulations provide legal frameworks that guide institutions in managing cyber risks, ensuring that they are held accountable for maintaining secure systems and data protection protocols. By adhering to regulatory requirements, financial institutions not only mitigate the risk of legal penalties but also enhance their cybersecurity maturity and operational resilience.

2.2 Cybersecurity Risks in Financial Institutions

In today's digital age, cybersecurity risks pose a significant challenge to financial institutions, which are prime targets for cybercriminals due to their valuable assets, sensitive customer data, and critical role in the global economy. Cybersecurity threats have evolved in sophistication, frequency, and impact, requiring financial organizations to develop robust security measures and stay ahead of emerging risks as shown in figure 1 (Jović and Nikolić, 2022) [32]. This explores the threat landscape facing financial institutions, the vulnerabilities specific to these organizations, and the multifaceted impact of cybersecurity risks on their operations and the broader economy.

Financial institutions face a wide variety of cybersecurity threats, each with the potential to cause severe damage. Among the most common and dangerous are phishing attacks, where cybercriminals use fraudulent emails or websites to steal login credentials or sensitive information. Malware is another prevalent threat, where malicious software is used to infiltrate systems and either steal data or disrupt operations (Bhadouria, 2022) [14]. Distributed Denial of Service (DDoS) attacks, which overload an institution's servers and cause service disruptions, are also frequent. These attacks not only affect customer experience but also result in significant financial losses.Perhaps the most concerning threats to financial institutions are Advanced Persistent Threats (APTs). APTs are highly sophisticated, prolonged cyberattacks where attackers remain inside the network, often undetected for long periods, to gather intelligence or sabotage operations. These types of attacks target critical infrastructure and can involve various tactics, including exploiting vulnerabilities and leveraging social engineering. As financial services become more digitized, the frequency and severity of these attacks continue to rise, posing an increasing threat to organizations

globally.Cyberattacks on financial institutions have become more frequent in recent years, driven by both technological advancements and an increase in cybercriminal activity. The global financial industry has witnessed a surge in ransomware attacks, where malicious actors demand payment in exchange for releasing stolen or encrypted data (Vardalaki and Vlachos, 2021) [65]. Furthermore, the use of artificial intelligence (AI) by cybercriminals is increasingly enabling them to launch more targeted, automated, and sophisticated attacks. The trend indicates that financial institutions will continue to face more complex and damaging cyber threats unless significant advancements in cybersecurity technologies are made (Pandey *et al*., 2022) [50].

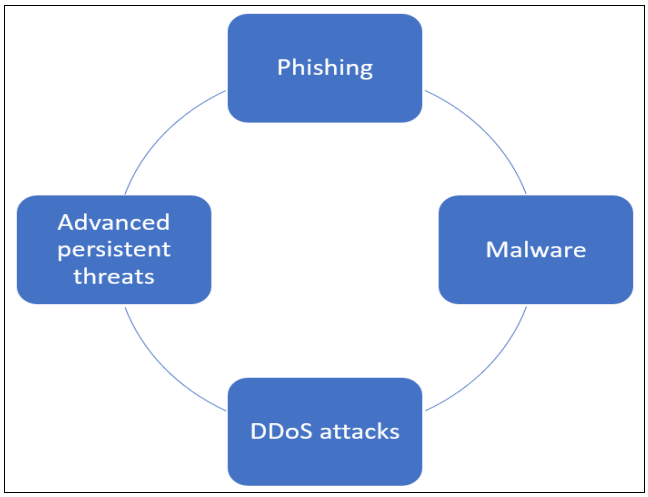

Fig 1: Types of cybersecurity threats

Financial institutions are particularly vulnerable to cybersecurity risks due to a variety of factors. One of the key vulnerabilities is the reliance on legacy systems and outdated security protocols. Many financial institutions continue to use outdated software and infrastructure that were designed before modern cybersecurity challenges emerged (Michalec *et al*., 2022) [44]. These legacy systems often lack the necessary defenses to withstand new threats and are ripe for exploitation by cybercriminals. Consequently, financial organizations must prioritize upgrading their systems to maintain strong defenses against increasingly advanced cyberattacks.Another significant vulnerability is the reliance on third-party vendors and supply chains. Many financial institutions engage with a wide range of third-party providers for services such as cloud storage, payment processing, and data analytics. While these partnerships provide operational efficiencies, they also introduce cybersecurity risks. A breach in a third-party vendor's system can result in a direct compromise of the financial institution's own systems, as demonstrated by high-profile supply chain attacks in other sectors. Ensuring the cybersecurity practices of third-party vendors align with industry standards is essential for mitigating this risk.Data privacy and protection are also major concerns within the financial sector. Financial institutions handle vast amounts of sensitive customer data, including personal identification, financial records, and transaction histories. Any breach of this data can lead to severe consequences, such as identity theft, fraud, and financial loss. As financial institutions embrace digital transformation and leverage technologies such as cloud computing, they must ensure their data protection practices meet stringent regulatory standards to safeguard customer privacy and prevent data breaches (Oyegbade *et al*., 2022) [46].

The consequences of cybersecurity risks in financial institutions can be devastating. Financial losses are perhaps the most direct and apparent impact, with breaches and attacks often leading to substantial financial penalties (Felbermayr *et al*., 2021) [26]. Additionally, legal liabilities associated with breaches can arise from lawsuits filed by affected customers or partners, which further increase financial strain.Reputational damage is another critical consequence of cybersecurity risks. Financial institutions are built on trust, and a cyberattack can erode this trust, leading to a loss of customers and business partners. Once a financial institution becomes a victim of a high-profile cyberattack, its brand image and customer confidence can be severely compromised. The long-term damage to a company's reputation may take years to recover from and can result in reduced market share, customer churn, and diminished business opportunities.Cyberattacks can also disrupt the day-to-day operations of financial institutions. In the event of a breach, organizations may need to suspend services temporarily while investigating and mitigating the damage. This disruption can delay transactions, halt business operations, and erode customer confidence. Furthermore, regulatory sanctions may follow, particularly in jurisdictions with stringent data protection and cybersecurity laws. Financial institutions that fail to meet compliance standards can face substantial fines, which exacerbate the operational and financial impacts of cyber incidents.On a larger scale, widespread cyber incidents in the financial sector can have a significant economic impact. Financial institutions play a critical role in the global economy, and a large-scale breach can lead to market instability, loss of investor confidence, and disruptions to international trade (Duran and Griffin, 2021) [23]. The interconnected nature of financial systems means that a breach in one institution can have a ripple effect across other organizations, industries, and even countries. This systemic risk could trigger a chain reaction, leading to broader economic consequences. Cybersecurity risks in financial institutions present complex and multifaceted challenges. The threat landscape continues to evolve, with cybercriminals using increasingly sophisticated methods to target financial organizations. Vulnerabilities such as legacy systems, third-party dependencies, and data privacy concerns make financial institutions particularly susceptible to cyberattacks. The impacts of cybersecurity breaches can range from financial losses and legal consequences to reputational damage and economic disruption. As the financial sector becomes more digitalized, organizations must prioritize cybersecurity measures to protect their assets, safeguard customer trust, and ensure stability in the broader economy.

2.3 Control Deficiencies in Cybersecurity Governance

Effective cybersecurity governance is essential for financial institutions to safeguard sensitive data, maintain operational stability, and ensure regulatory compliance (Krüger and Brauchle, 2021) [38]. However, many organizations face significant control deficiencies that weaken their cybersecurity posture and expose them to heightened risks. These deficiencies can be categorized into governance-level, operational, and technical deficiencies, each contributing to

vulnerabilities in the organization's overall security framework as shown in figure 2. This explores these deficiencies, examines their causes, and discusses methods for measuring and addressing them.

At the governance level, deficiencies often arise from a lack of clear cybersecurity policies and leadership. Financial institutions may have incomplete or vague policies that fail to outline specific cybersecurity objectives, roles, and responsibilities. Inadequate leadership or unclear accountability structures can hinder the effective execution of cybersecurity strategies, making it difficult to prioritize risk management or align cybersecurity efforts with broader organizational goals. Without strong cybersecurity governance, financial institutions struggle to establish a culture of security or respond effectively to evolving threats.Operational deficiencies often manifest in inadequate monitoring, poor incident response protocols, and ineffective vulnerability management (Dissanayake *et al*., 2022) [22]. Monitoring systems are crucial for detecting potential threats, but if these systems are not properly configured or regularly updated, they may fail to identify vulnerabilities or malicious activities in time. Similarly, an insufficient incident response framework can lead to slow or ineffective reactions when a breach occurs, exacerbating the damage caused by cyberattacks (Lehto, 2022) [39]. Vulnerability management deficienciessuch as delayed patching, unaddressed security gaps, and improper configurationcan leave systems exposed to known exploits. Effective operational cybersecurity processes must be continuous, adaptive, and timely to mitigate risks effectively.Technical deficiencies relate to the failure to implement robust access control mechanisms, inadequate encryption practices, and the use of outdated software. Weak or poorly managed access controls allow unauthorized users to gain access to sensitive data or systems, increasing the risk of breaches. Insufficient encryption of datawhether at rest or in transitleaves information vulnerable to interception by cybercriminals. Additionally, outdated software or hardware can introduce significant security vulnerabilities, as older systems may no longer receive security updates or patches. A failure to implement up-to-date, robust technical controls is a critical vulnerability that compromises the entire security framework.

One of the primary causes of control deficiencies in cybersecurity governance is resource constraints. Financial institutions often face budget limitations that restrict their ability to invest in comprehensive cybersecurity measures. In particular, the cost of acquiring advanced security tools, upgrading outdated infrastructure, and hiring skilled cybersecurity personnel can be prohibitive. As a result, organizations may struggle to maintain or improve their cybersecurity controls, leading to gaps in their governance frameworks. Budgetary constraints can also hinder the implementation of effective training programs for employees, leaving organizations vulnerable to social engineering and insider threats (Alsowail and Al-Shehari, 2022) [9]. Another significant cause of control deficiencies is the shortage of skilled cybersecurity professionals. The demand for cybersecurity experts far exceeds the supply, leading to difficulties in hiring and retaining qualified personnel. Many financial institutions lack the internal expertise required to design, implement, and maintain effective cybersecurity governance practices. This shortage of skilled professionals contributes to weak security controls, particularly in areas such as threat monitoring, incident response, and vulnerability management. Additionally, insufficient training of existing staff can result in ineffective implementation of cybersecurity protocols, which further exacerbates control deficiencies.A lack of alignment between IT and business objectives is also a key contributor to cybersecurity governance deficiencies. When cybersecurity policies and initiatives are not aligned with the institution's overall business strategy, security efforts can become fragmented or misdirected. This misalignment may result in inadequate investment in cybersecurity measures, weak risk management strategies, or the prioritization of operational efficiency over security. Ensuring that cybersecurity governance is integrated into the organization's broader business goals is crucial for developing a cohesive, effective approach to managing cyber risks.

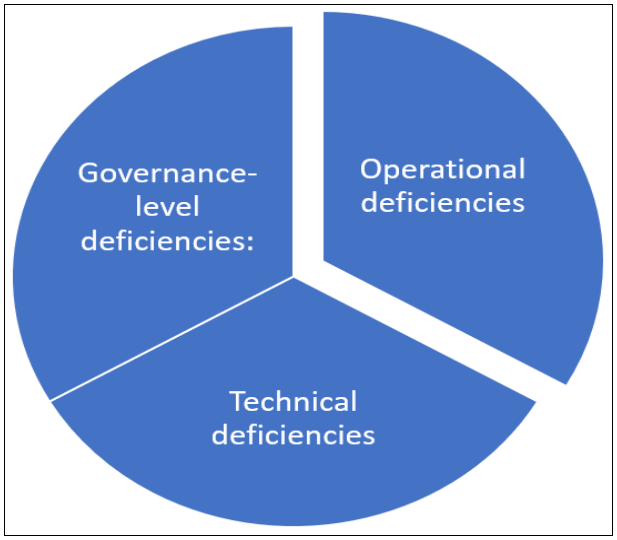

Fig 2: Types of Control Deficiencies

Measuring control deficiencies requires a systematic, quantitative approach that can accurately assess the effectiveness of cybersecurity measures. Surveys and audits are commonly used tools for gathering data on cybersecurity practices, identifying gaps in governance, and measuring compliance with established policies. Surveys can be used to assess employee awareness of cybersecurity policies, while audits can evaluate the implementation and effectiveness of security controls (Slapničar *et al*., 2022) [59]. Additionally, data analytics techniques can be employed to monitor system activity, track incidents, and identify vulnerabilities that may indicate deficiencies in cybersecurity governance.Key performance indicators (KPIs) and metrics are essential for evaluating the effectiveness of cybersecurity controls and identifying areas of weakness. Common metrics used to assess cybersecurity performance include breach frequency (the number of successful attacks or data breaches within a specific timeframe), response time (the time taken to identify and mitigate security incidents), and the number of unresolved system vulnerabilities. Other metrics, such as patch management effectiveness, incident recovery time, and access control violations, provide valuable insights into operational deficiencies. By regularly tracking these metrics, financial institutions can assess the state of their cybersecurity controls and make data-driven decisions about where improvements are

needed.Benchmarking is another effective method for measuring control deficiencies. By comparing an institution's cybersecurity practices against industry standards and best practices, such as those set by frameworks like NIST, ISO 27001, or COBIT, financial institutions can gain insights into where their governance models are lacking. Benchmarking allows institutions to identify gaps in their cybersecurity controls relative to peers or industry leaders, providing a clear picture of areas that require improvement (AlDaajeh *et al*., 2022) [5]. This process helps financial institutions prioritize their investments in cybersecurity and develop targeted strategies to address deficiencies.

2.4 Regulatory Compliance in Cybersecurity Governance

In the modern financial sector, the rapid digitalization of operations has significantly increased the exposure to cyber risks. Consequently, ensuring robust cybersecurity governance is crucial for financial institutions to mitigate potential threats. Regulatory compliance plays an essential role in this context, guiding institutions in maintaining security standards and protecting sensitive data (Karale, 2021) [33]. This explores the regulatory landscape for financial institutions, the challenges they face in achieving compliance, how adherence to regulations is measured, and the relationship between cybersecurity governance and regulatory compliance.

Financial institutions operate in a complex regulatory environment designed to ensure the security and stability of the sector. One of the key regulations impacting cybersecurity in the financial sector is the Sarbanes-Oxley Act (SOX), particularly Section 404, which mandates that publicly traded companies maintain adequate internal controls over financial reporting, including cybersecurity measures. SOX requires financial institutions to establish and regularly assess their internal control mechanisms, ensuring they are capable of safeguarding sensitive financial data from unauthorized access or breaches.Another significant regulation is Basel III, which provides a framework for banks and other financial institutions to manage risks, including those associated with cybersecurity (Koto *et al*., 2021) [37]. Basel III emphasizes the importance of maintaining robust risk management systems, which incorporate cybersecurity as part of the operational risk management process. Institutions must comply with these standards to ensure their resilience to cyber threats that could compromise financial stability.

In the United States, Dodd-Frank Wall Street Reform and Consumer Protection Act also has provisions that influence cybersecurity governance. Dodd-Frank focuses on enhancing transparency, risk management, and consumer protection. Financial institutions are required to establish cybersecurity risk management programs that address emerging risks, such as advanced persistent threats (APTs), and ensure compliance with the Consumer Financial Protection Bureau's regulations regarding data privacy (Keskin *et al*., 2021; Ozarslan, 2022) [35, 47]. Internationally, various compliance standards and frameworks guide cybersecurity governance. The General Data Protection Regulation (GDPR), established by the European Union, imposes stringent rules on the handling and protection of personal data. Financial institutions operating in the EU or with EU clients must comply with GDPR, which includes requirements for data breach notifications and penalties for failure to comply. Additionally, ISO/IEC 27001 provides a globally recognized framework for information security management systems (ISMS), ensuring that financial institutions establish a systematic approach to protecting sensitive data and reducing cybersecurity risks.

Achieving compliance with these regulations is a complex and often resource-intensive process for financial institutions. One of the significant challenges is the complexity of regulatory requirements and the frequent updates to cybersecurity frameworks (Markopoulou and Papakonstantinou, 2021) [41]. Regulations such as SOX, Basel III, and GDPR are continuously evolving to address new and emerging threats, requiring financial institutions to invest considerable time and effort in ensuring they remain up-to-date with regulatory changes. As cybersecurity risks evolve, regulations must also adapt, which can lead to frequent updates and changes to compliance requirements.Another challenge is the gaps in compliance programs, often arising due to limited resources or poor governance. Smaller financial institutions or those operating in regions with fewer regulatory oversight may struggle to dedicate the necessary financial and human resources to m*eet all* compliance requirements. This can lead to incomplete compliance programs, where certain aspects of cybersecurity governance are neglected or inadequately implemented, leaving institutions vulnerable to cyber threats and potential regulatory sanctions.Furthermore, poor governance and inadequate oversight can contribute to compliance failures. Institutions may lack a clear framework for managing compliance, and key stakeholders may not fully understand their responsibilities or the importance of regulatory adherence (Abbott and Snidal, 2021) [1]. This gap can result in inconsistent application of policies, weak enforcement of cybersecurity practices, and a general failure to maintain an effective security posture.

Measuring adherence to regulatory requirements is essential for ensuring that financial institutions comply with cybersecurity standards. Compliance audits and assessments are fundamental tools used to evaluate the effectiveness of an institution's cybersecurity governance (Maleh *et al*., 2021) [40]. These audits typically involve a detailed examination of an institution's systems, policies, and procedures to determine whether they align with the regulatory requirements. Regular internal and external audits help identify potential gaps in compliance and allow institutions to address them proactively before regulatory authorities intervene.

Failure to comply with cybersecurity regulations can lead to penalties and fines, which can be both financially damaging and detrimental to an institution's reputation. Case studies such as the Equifax data breach in 2017 highlight the severe consequences of non-compliance with data protection regulations. Equifax faced not only significant financial penalties but also a loss of consumer trust due to inadequate cybersecurity measures, which ultimately led to the exposure of millions of sensitive records. Similarly, the Target breach in 2013 resulted in substantial fines and a tarnished reputation for failing to meet data security standards, further illustrating the high stakes of regulatory non-compliance in the financial sector.

Effective cybersecurity governance is crucial for ensuring regulatory compliance. Well-structured governance frameworks help financial institutions establish policies,

procedures, and practices that align with both industry standards and regulatory requirements. This alignment ensures that cybersecurity risks are adequately managed, and data privacy is prioritized, reducing the likelihood of breaches and non-compliance.Cybersecurity policies play a central role in meeting regulatory requirements (Srinivas *et al*., 2019) [60]. These policies ensure that personal data is collected, processed, stored, and shared in a manner that complies with data protection regulations, thereby mitigating the risk of fines for non-compliance. Additionally, regular incident reporting and breach notification procedures are essential for ensuring financial institutions meet requirements outlined in regulations such as GDPR and the NYDFS Cybersecurity Regulation, which mandates timely reporting of cyber incidents.Furthermore, cybersecurity governance frameworks help institutions implement continuous monitoring, testing, and updating of their security practices, which is crucial for adhering to regulations that require ongoing risk management (Henderson, 2021; Mishra *et al*., 2022) [31, 45]. Establishing a culture of compliance and security awareness within the organization also plays a vital role in maintaining regulatory adherence and ensuring that all stakeholders, from IT professionals to senior management, understand and prioritize compliance.

2.5 Quantitative Analysis of Control Deficiencies and Regulatory Compliance

The growing complexity and sophistication of cyber threats have made it essential for financial institutions to establish robust cybersecurity governance frameworks (Kaur *et al*., 2021) [34]. However, many organizations continue to experience control deficiencies that hinder effective risk management and regulatory compliance. A quantitative analysis of these deficiencies provides valuable insights into the relationship between control gaps, regulatory adherence, and cybersecurity risks. This explores the data collection methodology, key performance indicators (KPIs), statistical techniques, and findings that highlight the connection between control deficiencies and regulatory compliance in the context of cybersecurity governance.

The first step in a quantitative analysis of control deficiencies and regulatory compliance is designing an effective data collection methodology as shown in figure 3. Surveys play a crucial role in gathering information from key stakeholders in financial institutions, such as cybersecurity professionals, compliance officers, and IT managers (Wong *et al*., 2022) [69]. These surveys are designed to assess the current state of cybersecurity governance, including the implementation of policies, the adequacy of security controls, and the institution's approach to regulatory compliance. By targeting professionals in positions of responsibility, the survey can yield insights into areas where governance practices are strong or weak, offering a comprehensive view of the cybersecurity posture across institutions.

In addition to surveys, interviews and case studies provide more in-depth insights into the experiences of financial institutions with varying levels of cybersecurity governance (Varga *et al*., 2021) [66]. Case studies from organizations with strong governance practices can serve as models for other institutions, while those with weak governance practices highlight areas that require urgent attention. Through interviews, cybersecurity experts can provide qualitative data on the specific challenges they face, such as limited resources, lack of training, or inadequate tools. Case studies and interviews also help identify the root causes of control deficiencies and their impact on regulatory compliance, providing a more nuanced understanding of the issue.Data sources for this analysis include audits, vulnerability reports, and industry benchmarks. Audits provide an objective assessment of an institution's cybersecurity controls, highlighting gaps in policy implementation and control effectiveness. Vulnerability reports give insight into the number and severity of system weaknesses, helping institutions identify areas of improvement (Anwar *et al*., 2021) [10]. Industry benchmarks, such as those from NIST or ISO 27001, provide comparative data on best practices, allowing institutions to measure their performance relative to industry standards.

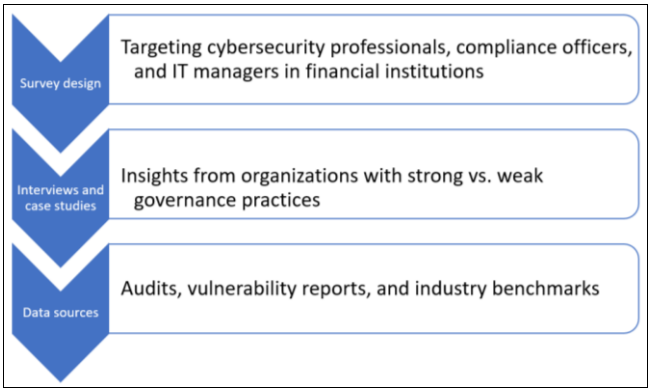

Fig 3: Data collection methodology

Key performance indicators (KPIs) are essential for quantitatively evaluating control deficiencies in cybersecurity governance. One important control deficiency indicator is the number of unresolved vulnerabilities within an organization's systems. Vulnerabilities that remain unpatched or inadequately managed create significant security risks, and their persistence is often a direct indicator of poor governance (Ulven and Wangen, 2021) [64]. Another KPI is incident response times—the time it takes for an organization to detect, respond to, and recover from a cybersecurity incident. Longer response times typically reflect gaps in incident response protocols or inadequate staffing and resources. Additionally, audit findings can serve as an indicator of control deficiencies, as audits often identify non-compliance with internal policies or regulatory requirements, signaling potential weaknesses in governance.In addition to control deficiencies, compliance indicators offer insight into the institution's ability to meet regulatory requirements. A critical compliance KPI is the percentage of regulations met, which tracks the extent to which financial institutions comply with cybersecurity-related regulations such as GDPR, GLBA, or PCI DSS (Ahmed, 2022) [4]. Another important compliance indicator is the number of non-compliance incidents, which measures the frequency of failures to meet regulatory standards. Non-compliance can result in penalties, fines, and reputational damage. The cost of non-compliance is also a vital KPI, as it quantifies the financial and operational consequences of failing to meet regulatory requirements, including the costs of legal penalties, customer compensation, and reputational recovery efforts.

Descriptive statistics are useful for identifying common control deficiencies across a sample of financial institutions (Vo *et al*., 2021) [67]. By summarizing the frequency and distribution of deficiencies, descriptive statistics provide an overview of the most prevalent issues in cybersecurity governance. For example, the percentage of institutions reporting weak access control or outdated software can help highlight widespread vulnerabilities. Descriptive statistics also allow researchers to categorize deficiencies by severity, aiding in the prioritization of cybersecurity improvements.Correlation analysis can help link control deficiencies with regulatory non-compliance and cybersecurity risks. By examining the relationship between specific deficienciessuch as inadequate vulnerability management—and the likelihood of non-compliance, correlation analysis provides a clearer understanding of how governance gaps influence regulatory outcomes. Additionally, correlation analysis can reveal how deficiencies in one area (e.g., incident response) can lead to increased cybersecurity risks, such as data breaches or financial losses (Algarni*et al*., 2021).Regression analysis is a powerful statistical technique used to predict the likelihood of achieving compliance based on specific governance practices and control maturity. By analyzing data on various governance factors (e.g., leadership, training, resource allocation) and control measures (e.g., encryption, access control), regression models can predict the effectiveness of different governance strategies in achieving regulatory compliance. Regression analysis can also identify key predictors of cybersecurity risks, providing financial institutions with actionable insights on which practices most effectively mitigate these risks.

The quantitative analysis reveals several common control deficiencies across financial institutions (Damşa *et al*., 2021) [20]. These include weaknesses in incident response protocols, ineffective vulnerability management practices, and outdated software systems. The persistence of these deficiencies indicates systemic issues in the governance structures of many organizations, which may be caused by resource limitations, lack of expertise, or poor alignment between IT and business objectives. Addressing these deficiencies is critical to improving the overall cybersecurity posture of financial institutions.The analysis demonstrates a clear correlation between control deficiencies and failure to meet regulatory standards (Pan and Tang, 2021) [49]. Institutions with significant control gaps, particularly in areas such as access control, encryption, and vulnerability management, were more likely to experience non-compliance incidents. This relationship underscores the importance of effective governance in ensuring that cybersecurity efforts are aligned with regulatory requirements and industry standards.

The analysis also suggests that improvements in governance practices lead to better regulatory compliance and reduced cybersecurity risks. Institutions that invested in strengthening their governance frameworkssuch as adopting IT governance frameworks like NIST or ISO 27001—tended to have fewer non-compliance incidents and better overall risk management. These institutions were also more adept at responding to cybersecurity threats and mitigating potential breaches, highlighting the critical role of strong governance in enhancing institutional resilience.

2.6 Strategies for Enhancing Cybersecurity Governance

In an era where cyber threats are increasing in sophistication and frequency, financial institutions, businesses, and government organizations must prioritize cybersecurity governance to safeguard their operations, sensitive data, and customer trust (Fouad, 2021; Cheryl and Ng, 2022) [28, 19]. A robust cybersecurity governance strategy helps institutions not only defend against cyberattacks but also stay compliant with regulations, manage risk, and foster a security-conscious organizational culture. This outlines several critical strategies for enhancing cybersecurity governance, focusing on strengthening IT governance frameworks, addressing control deficiencies, improving regulatory compliance, building a cybersecurity culture, and ensuring continuous monitoring and improvement.

A critical first step in enhancing cybersecurity governance is the establishment of clear leadership roles and responsibilities. One of the most effective ways to manage cybersecurity risks is by designating a Chief Information Security Officer (CISO) or an equivalent leadership position. The CISO is responsible for overseeing the entire cybersecurity program, from risk assessments to incident management (Sandhu, 2021) [55]. The CISO ensures that cybersecurity is not treated as a siloed IT function but is integrated into the broader organizational strategy. This position also serves as the primary point of contact for senior executives and the board of directors on cybersecurity matters, facilitating clear communication and enabling informed decision-making.Another key aspect of strengthening IT governance is aligning cybersecurity strategies with organizational goals and risk management frameworks. Financial institutions and other organizations must ensure that their cybersecurity strategies are not only reactive but proactive, identifying potential risks that may impact organizational objectives. This alignment ensures that cybersecurity is seen as an enabler of business success rather than a hindrance to organizational goals.

Control deficiencies are a significant challenge to cybersecurity governance. Financial institutions and organizations must prioritize addressing these gaps to build a resilient security posture (Pacthod *et al*., 2022) [48]. One of the primary ways to address control deficiencies is by investing in cybersecurity training, tools, and resources. Ensuring that employees are well-equipped with the right knowledge and tools to identify and respond to cyber threats is critical. Regular cybersecurity training programs should be mandatory for all employees, including those in non-technical roles. Training should cover topics such as phishing detection, secure data handling, and the use of strong authentication methods.In addition to training, institutions must also enhance incident response protocols and risk monitoring systems. An effective incident response plan ensures that when a cyberattack or breach occurs, the organization can respond quickly and minimize the damage. This involves having a clear plan for identifying, containing, and recovering from incidents. Furthermore, risk monitoring systems should be put in place to continuously track vulnerabilities and emerging threats. Early detection of potential threats allows organizations to respond proactively, preventing attacks before they escalate (Raza, 2021) [54]. Another essential strategy to address control deficiencies is conducting regular vulnerability assessments and

penetration testing. Vulnerability assessments help identify potential weaknesses in an organization's systems and networks, while penetration testing simulates real-world cyberattacks to evaluate the effectiveness of existing defenses. These assessments provide valuable insights into areas where the organization's security may be lacking and allow the organization to implement necessary improvements before vulnerabilities are exploited by cybercriminals (Armenia *et al*., 2021; Georgiadou *et al*., 2021) [11, 29].

Cybersecurity governance is not only about protecting systems and data but also ensuring that organizations comply with relevant regulations and standards (Bechara and Schuch, 2021) [13]. Regulatory compliance is an essential component of a sound cybersecurity strategy. Streamlining compliance processes with automated tools and reporting systems can significantly improve the efficiency of compliance efforts. Automated tools help institutions track changes in regulations, assess compliance gaps, and ensure that they are consistently meeting their legal obligations. Reporting systems also streamline the process of providing regulators with the necessary documentation and evidence of compliance.Regular internal and external audits are also crucial to assess compliance levels. Audits should be conducted frequently to identify areas where the institution may be falling short of compliance standards (Earnhart and Harrington, 2021) [24]. Internal audits ensure that cybersecurity policies and procedures are being followed, while external audits by third-party experts offer an objective assessment of an organization's compliance status. Engaging with auditors and stakeholders helps financial institutions identify weaknesses in their governance processes and resolve compliance issues before they result in penalties or reputational damage.In addition, financial institutions should engage with regulators and industry groups to stay informed about evolving cybersecurity standards and best practices. Cybersecurity regulations are constantly evolving to address emerging threats, and being proactive in maintaining relationships with regulatory bodies and industry groups ensures that organizations are well-positioned to adapt to new requirements. Regular participation in cybersecurity forums and conferences also helps organizations stay up to date on best practices, emerging risks, and evolving technologies (Sun *et al*., 2022) [61].

Building a cybersecurity culture within an organization is essential for ensuring long-term success in managing cybersecurity risks. A strong cybersecurity culture empowers employees at all levels to take responsibility for protecting sensitive data and systems. Promoting a culture of cybersecurity awareness involves creating an environment where security is ingrained in the organization's values, not just a technical requirement (Fisher *et al*., 2021) [27]. Organizations should ensure that cybersecurity is discussed regularly at all levels, from the executive board to individual employees.Employee training and awareness programs are a key part of fostering a cybersecurity culture. These programs should focus on reducing human error-related breaches, which remain one of the most common causes of security incidents. Training should educate employees about recognizing phishing emails, understanding the importance of strong password practices, and reporting suspicious activities. By instilling a sense of shared responsibility and ensuring that every employee is part of the organization's cybersecurity efforts, financial institutions can reduce the likelihood of breaches caused by negligence or lack of awareness.

Cybersecurity governance is a dynamic process that requires continuous monitoring and improvement. One of the most effective ways to enhance cybersecurity is by implementing continuous monitoring of cybersecurity controls and systems (Ali, 2021) [8]. This approach enables organizations to detect threats in real-time and respond quickly to mitigate potential damage. Continuous monitoring can include real-time analysis of network traffic, behavior analytics, and the use of intrusion detection systems to identify anomalies that may indicate a breach.Additionally, cybersecurity policies should be regularly updated and improved based on emerging threats and regulatory changes. Cybersecurity governance is not a one-time initiative but an ongoing process that requires adaptation to new technologies, threats, and compliance requirements (Khan and Liu, 2022; Falco and Rosenbach, 2022) [36, 25]. By establishing a continuous feedback loop and regularly reviewing security measures, organizations can ensure their cybersecurity posture remains robust and effective.

3. Conclusion

The analysis highlights a clear connection between control deficiencies, cybersecurity risks, and regulatory compliance in financial institutions. Institutions that exhibit significant governance gaps, particularly in areas like incident response, vulnerability management, and access control, are more likely to experience regulatory non-compliance and increased cybersecurity risks. Weak cybersecurity governance practices exacerbate vulnerabilities, leaving institutions exposed to data breaches, financial losses, and reputational damage. Conversely, institutions with robust governance frameworks demonstrate better regulatory adherence and resilience to cyber threats. Strong cybersecurity governance not only protects against immediate threats but also ensures long-term institutional stability by aligning security measures with business objectives and regulatory requirements.

To address the challenges identified, financial institutions must prioritize investment in cybersecurity governance and regulatory compliance. This includes adopting recognized IT governance frameworks (e.g., NIST, ISO 27001) and continuously updating security protocols to address evolving threats. Furthermore, developing a culture of continuous improvement and proactive risk management is essential. This involves regular cybersecurity training, periodic audits, and updates to incident response plans to ensure preparedness for emerging threats. Financial institutions should also engage in benchmarking exercises to assess their cybersecurity practices against industry standards, identifying areas for improvement and maintaining alignment with regulatory requirements.

The regulatory landscape surrounding cybersecurity is constantly evolving, and financial institutions must adapt to meet new and more stringent requirements. Future trends indicate that regulations will likely become more comprehensive and detailed, with an increased focus on data privacy, threat intelligence sharing, and secure cloud infrastructures. Additionally, emerging cybersecurity threats, such as advanced persistent threats (APTs), ransomware, and AI-driven cyberattacks, will necessitate adaptive governance models that are flexible and resilient.

Financial institutions will need to implement dynamic and forward-looking cybersecurity frameworks to stay ahead of these threats while maintaining compliance with an increasingly complex regulatory environment.

4. References

1. Abbott KW, Snidal D. The governance triangle: Regulatory standards institutions and the shadow of the state. In The spectrum of international institutions (pp. 52-91). Routledge, 2021.
2. Abrahams TO, Ewuga SK, Kaggwa S, Uwaoma PU, Hassan AO, Dawodu SO. Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. World Journal of Advanced Research and Reviews. 2023; 20(3):1743-1756.
3. Adrian FX, Wang GUNAWAN. Measure the Level Capability IT Governance in Effectiveness Internal Control for Cybersecurity Using the COBIT 2019 in Organization: Banking Company. Journal of Theoretical and Applied Information Technology. 2023; 15(5).
4. Ahmed NB. Cybersecurity in Healthcare System: Evaluation and Assessment of the Cybersecurity readiness of Mobile Field Hospital's Resilience (Doctoral dissertation, IMT-MINES ALES-IMT-Mines Alès Ecole Mines-Télécom), 2022.
5. AlDaajeh S, Saleous H, Alrabaee S, Barka E, Breitinger F, Choo KKR. The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security. 2022; 119:102754.
6. Aldboush HH, Ferdous M. Building trust in fintech: An analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. International Journal of Financial Studies. 2023; 11(3):90.
7. Algarni AM, Thayananthan V, Malaiya YK. Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems. Applied Sciences. 2021; 11(8):3678.
8. Ali S. Cybersecurity management for distributed control system: Systematic approach. Journal of Ambient Intelligence and Humanized Computing. 2021; 12(11):10091-10103.
9. Alsowail RA, Al-Shehari T. Techniques and countermeasures for preventing insider threats. PeerJ Computer Science. 2022; 8:e938.
10. Anwar A, Abusnaina A, Chen S, Li F, Mohaisen D. Cleaning the NVD: Comprehensive quality assessment, improvements, and analyses. IEEE Transactions on Dependable and Secure Computing. 2021; 19(6):4255-4269.
11. Armenia S, Angelini M, Nonino F, Palombi G, Schlitzer MF. A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems. 2021; 147:113580.
12. Aslam M, Khan Abbasi MA, Khalid T, Shan RU, Ullah S, Ahmad T, *et al*. Getting smarter about smart cities: Improving data security and privacy through compliance. Sensors. 2022; 22(23):9338.
13. Bechara FR, Schuch SB. Cybersecurity and global regulatory challenges. Journal of Financial Crime. 2021; 28(2):359-374.
14. Bhadouria AS. Study of: Impact of malicious attacks and data breach on the growth and performance of the company and few of the world's biggest data breaches. International Journal of Scientific and Research Publications. 2022; 10(10):1-11.
15. Bhutta MNM, Bhattia S, Alojail MA, Nisar K, Cao Y, Chaudhry SA, *et al*. Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS). Wireless communications and mobile computing. 2022; 2022(1):9942270.
16. Boeding M, Boswell K, Hempel M, Sharif H, Lopez Jr J, Perumalla K. Survey of cybersecurity governance, threats, and countermeasures for the power grid. Energies. 2022; 15(22):8692.
17. Bokan B, Santos J. April. Managing cybersecurity risk using threat based methodology for evaluation of cybersecurity architectures. In 2021 Systems and Information Engineering Design Symposium (SIEDS) (pp. 1-6). IEEE, 2021.
18. Bongiovanni I, Renaud K, Brydon H, Blignaut R, Cavallo A. A quantification mechanism for assessing adherence to information security governance guidelines. Information & Computer Security. 2022; 30(4):517-548.
19. Cheryl BK, Ng BK. Protecting the unprotected consumer data in internet of things: Current scenario of data governance in Malaysia. Sustainability. 2022; 14(16):9893.
20. Damşa C, Langford M, Uehara D, Scherer R. Teachers' agency and online education in times of crisis. Computers in human behavior. 2021; 121:106793.
21. Darem AA, Alhashmi AA, Alkhaldi TM, Alashjaee AM, Alanazi SM, Ebad SA. Cyber threats classifications and countermeasures in banking and financial sector. IEEe Access. 2023; 11:125138-125158.
22. Dissanayake N, Zahedi M, Jayatilaka A, Babar MA. Why, how and where of delays in software security patch management: An empirical investigation in the healthcare sector. Proceedings of the ACM on Human-computer Interaction. 2022; 6(CSCW2):1-29.
23. Duran RE, Griffin P. Smart contracts: Will Fintech be the catalyst for the next global financial crisis? Journal of Financial Regulation and Compliance. 2021; 29(1):104-122.
24. Earnhart D, Harrington DR. Effects of audit frequency, audit quality, and facility age on environmental compliance. Applied Economics. 2021; 53(28):3234-3252.
25. Falco GJ, Rosenbach E. Confronting cyber risk: An embedded endurance strategy for cybersecurity. Oxford University Press, 2022.
26. Felbermayr G, Morgan TC, Syropoulos C, Yotov YV. Understanding economic sanctions: Interdisciplinary perspectives on theory and evidence. European Economic Review. 2021; 135:103720.
27. Fisher R, Porod C, Peterson S. Motivating employees and organizations to adopt a cybersecurity-focused culture. Journal of Organizational Psychology. 2021; 21(1):114-131.
28. Fouad NS. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy. 2021; 6(2):137-154.

29. Georgiadou A, Mouzakitis S, Askounis D. Assessing mitreatt&ck risk using a cyber-security culture framework. Sensors. 2021; 21(9):3267.
30. Haber MJ, Chappell B, Hills C. Regulatory compliance. In Cloud attack vectors: Building effective cyber-defense strategies to protect cloud resources (pp. 297-373). Berkeley, CA: Apress, 2022.
31. Henderson C. The United Nations and the regulation of cyber-security. Research Handbook on International Law and Cyberspace, 2021, 582-614.
32. Jović Ž, Nikolić I. The darker side of FinTech: the emergence of new risks. Zagreb International Review of Economics & Business. 2022; 25(SCI):46-63.
33. Karale A. The challenges of IoT addressing security, ethics, privacy, and laws. Internet of Things. 2021; 15:100420.
34. Kaur G, Lashkari ZH, Lashkari AH. Understanding cybersecurity management in FinTech. Springer International Publishing, 2021.
35. Keskin OF, Caramancion KM, Tatar I, Raza O, Tatar U. Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. Electronics. 2021; 10(10):1168.
36. Khan J, Liu Y. Data Privacy and Security Issues in Digital Transformation Initiatives. Journal of Emerging Technology and Digital Transformation. 2022; 1(1):33-42.
37. Koto C, Smith RJ, Schutte B. Cyber risk management frameworks for the South African banking industry. International Conference on Public Administration and Development Alternatives (IPADA), 2021.
38. Krüger PS, Brauchle JP. The European Union, cybersecurity, and the financial sector: A primer. Washington, DC, 2021.
39. Lehto M. Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection (pp. 3-42). Cham: Springer International Publishing, 2022.
40. Maleh Y, Sahid A, Belaissaoui M. A maturity framework for cybersecurity governance in organizations. EDPACS. 2021; 63(6):1-22.
41. Markopoulou D, Papakonstantinou V. The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. Computer law & security review. 2021; 41:105502.
42. Marotta A, Madnick S. Convergence and divergence of regulatory compliance and cybersecurity. Issues in Information Systems. 2021; 22(1).
43. Melaku HM. A dynamic and adaptive cybersecurity governance framework. Journal of Cybersecurity and Privacy. 2023; 3(3):327-350.
44. Michalec O, Milyaeva S, Rashid A. When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures? Big Data & Society. 2022; 9(1):20539517221108369.
45. Mishra A, Alzoubi YI, Anwar MJ, Gill AQ. Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security. 2022; 120:102820.
46. Oyegbade IK, Igwe AN, Ofodile OC, Azubuike C. Transforming financial institutions with technology and strategic collaboration: Lessons from banking and capital markets. Int J Multidiscip Res Growth Eval. 2022; 4(6):1118-27.
47. Ozarslan S. Key threats and cyber risks facing financial services and banking firms in 2022, 2022. URL: https://www. picussecurity. com/keythreats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022.
48. Pacthod D, Schive M, Smit S. White Paper Resilience for sustainable, inclusive growth, 2022.
49. Pan D, Tang J. The effects of heterogeneous environmental regulations on water pollution control: Quasi-natural experimental evidence from China. Science of the total environment. 2021; 751:141550.
50. Pandey AB, Tripathi A, Vashist PC. A survey of cyber security trends, emerging technologies and threats. Cyber security in intelligent computing and communications, 2022, 19-33.
51. Paul E, Callistus O, Somtobe O, Esther T, Somto K, Clement O, *et al*. Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. International Journal on Soft Computing. 2023; 14(3):01-16.
52. Yusif S, Hafeez-Baig A. A conceptual model for cybersecurity governance. Journal of applied security research. 2021; 16(4):490-513.
53. Perwej Y, Abbas SQ, Dixit JP, Akhtar N, Jaiswal AK. A systematic literature review on the cyber security. International Journal of scientific research and management. 2021; 9(12):669-710.
54. Raza H. Proactive cyber defense with AI: Enhancing risk assessment and threat detection in cybersecurity ecosystems. Journal Name Missing, 2021.
55. Sandhu JS. Cybersecurity for executives: Advancing leaders to practical cyber risk management. Notion Press, 2021.
56. Savaş S, Karataş S. Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. International Cybersecurity Law Review. 2022; 3(1):7-34.
57. Shinde N, Kulkarni P. Cyber incident response and planning: A flexible approach. Computer Fraud & Security. 2021; 2021(1):14-19.
58. Shukla S, George JP, Tiwari K, Kureethara JV. Data security. In Data ethics and challenges (pp. 41-59). Singapore: Springer Singapore, 2022.
59. Slapničar S, Vuko T, Čular M, Drašček M. Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems. 2022; 44:100548.
60. Srinivas J, Das AK, Kumar N. Government regulations in cyber security: Framework, standards and recommendations. Future generation computer systems. 2019; 92:178-188.
61. Sun N, Li CT, Chan H, Islam MZ, Islam MR, Armstrong W. How do organizations seek cyber assurance? Investigations on the adoption of the common criteria and beyond. Ieee Access. 2022; 10:71749-71763.
62. Thomas G, Sule MJ. A service lens on cybersecurity continuity and management for organizations' subsistence and growth. Organizational Cybersecurity Journal: Practice, Process and People. 2023; 3(1):18-40.

63. Uddin MH, Ali MH, Hassan MK. Cybersecurity hazards and financial system vulnerability: A synthesis of literature. Risk Management. 2020; 22(4):239-309.
64. Ulven JB, Wangen G. A systematic review of cybersecurity risks in higher education. Future Internet. 2021; 13(2):39.
65. Vardalaki A, Vlachos V. Emerging malware threats: The case of ransomware. In Cybersecurity Issues in Emerging Technologies (pp. 153-170). CRC Press, 2021.
66. Varga S, Brynielsson J, Franke U. Cyber-threat perception and risk management in the Swedish financial sector. Computers & security. 2021; 105:102239.
67. Vo DH, Nguyen NT, Van LTH. Financial inclusion and stability in the Asian region using bank-level data. Borsa Istanbul Review. 2021; 21(1):36-43.
68. Wang S, Asif M, Shahzad MF, Ashfaq M. Data privacy and cybersecurity challenges in the digital transformation of the banking sector. Computers & security. 2024; 147:104051.
69. Wong LW, Lee VH, Tan GWH, Ooi KB, Sohal A. The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. International Journal of Information Management. 2022; 66:102520.