Applying Systems thinking for Cyber Security Risk Management as part of Enterprise Risk Management Program for Stock and Derivatives Exchanges and Designated Clearing Organizations

by

Harish Jayabalan, BE, MS, MBA

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

August, 2026

Applying Systems thinking for Cyber Security Risk Management as part of Enterprise Risk Management Program for Stock/Derivatives Exchanges and Designated Clearing Organizations

by

Harish Jayabalan

APPROVED BY

Ivo Bulyubasic

Chair

Dedication

To my beloved grandmother, parents, uncles and aunts — your values, sacrifices, and unconditional love laid the foundation for who I am. Your guidance continues to shape my character, values and this accomplishment stands as a testament to the strength, wisdom, and resilience you instilled in me.

To Geetha—your unwavering support, patience, and grace carried our family through every step of our journey. While managing your own demanding career and our family, you made countless sacrifices so I could pursue mine. To Parth—your grit and drive in consistently achieving your goals inspired me deeply and gave me strength during the most challenging moments. To Krish—your curiosity, thoughtful questions, creativity, and warm hugs brought balance, joy, and perspective when I needed it most.

To Ashish and Ganga — your friendship and relentless pursuit of excellence in your respective fields sets a standard I truly respect, admire and get inspired by. To Dabholkar Uncle; your example of professional excellence during my formative years left a lasting impression. Seeing Akshay carry forward that legacy through his own academic and professional achievements has only deepened that admiration.

To Sanjana's parents and Pallavi; your academic brilliance and continued professional growth continue to motivate me with every step you take.

This work is dedicated to all of you and many others, with deep gratitude and love.

Acknowledgements

I would like to express my heartfelt gratitude to my thesis guide for the mentorship, insight, and steadfast encouragement throughout this academic journey. The guidance was essential in shaping both the structure and substance of this work. I am deeply thankful to my industry peers and coworkers for their patience, flexibility, and support, which enabled me to manage professional responsibilities while pursuing this milestone. A special note of appreciation goes to Doug, Matt, Randy, Steve and Eric; more than just trusted industry professionals and experts, you have been my trusted advisor, teacher and friend. Your insights, humor, and encouragement not only guided my thinking but also lightened the load during challenging times. I also wish to acknowledge many other professionals whose shared experiences and thoughtful discussions helped ground this research in real-world relevance. Each of you contributed meaningfully, and I am sincerely grateful for your support along the way.

ABSTRACT

< Applying Systems thinking for Cyber Security Risk Management as part of Enterprise Risk Management Program for Stock/Derivatives Exchanges and Designated Clearing Organizations>

<Harish Jayabalan>

<2026>

Dissertation Chair: <Chair's Name>

Co-Chair: <If applicable. Co-Chair's Name>

TABLE OF CONTENTS

Abstract

This research explores how Critical Success Factors (CSFs), applied through a systems thinking lens, can enhance cybersecurity risk governance within an Enterprise Risk Management (ERM) framework. Based on interviews with cybersecurity, risk, and compliance professionals, the study finds that CSFs—when clearly defined, quantitatively measured, and mapped to business processes, systems, and third-party dependencies—serve as effective tools for aligning cybersecurity controls with strategic objectives. Embedding CSFs into DevSecOps (DevSecOps is a development practice that integrates security initiatives at every stage of the software development lifecycle to deliver secure and robust applications) pipelines, regulatory disclosures, and board-level dashboards enables organizations to create dynamic feedback loops that continuously adjust risk posture in response to evolving threats. The study highlights the importance of cross-functional cyber risk committees, scenario-based planning, and cultural alignment to ensure shared accountability across the enterprise. Regulatory drivers such as the SEC's (US Regulators – Securities Exchange Commission) cybersecurity disclosure rules and Regulation SCI further reinforce the value of CSF-led governance. Ultimately, the research offers a practical model for converting abstract cyber risk into actionable, measurable, and enterprise-aligned controls—transforming cybersecurity from a technical silo into a strategic business enabler.

CHAPTER I

1. INTRODUCTION

Sterman (2000) offers a foundational perspective on systems thinking, emphasizing its relevance for understanding and managing complexity in dynamic organizational environments. He argues that most decision failures stem not from lack of data but from mental models that ignore feedback loops, time delays, and non-linear relationships within systems. Through system dynamics modeling, Sterman illustrates how reinforcing and balancing feedback structures drive long-term behavior, often in counterintuitive ways. These insights directly inform enterprise risk management by revealing how isolated risk controls can create unintended consequences if system interdependencies are ignored. As applied to ERM, Sterman's framework supports a shift from reactive, siloed risk assessments to integrated, adaptive processes that respond to complexity with continuous learning and systemic foresight.

1.1 The Role of Cybersecurity in Financial Market Stability

The efficient operation of capital markets relies heavily on the robustness of stock exchanges and designated clearing organizations. These institutions ensure market stability by facilitating transactions and mitigating financial risks. However, the increasing sophistication of cyber threats, coupled with the complex nature of financial markets, necessitates an integrated approach to cybersecurity risk management (Krueger, 2006). Russo et al. (2002) provide a comparative analysis of the development of clearing and central counterparty (CCP) services for exchange-traded derivatives in the U.S. and Europe, highlighting how structural, legal, and regulatory environments shaped different

evolutionary paths. The U.S. model emphasized early consolidation and strong regulatory oversight, while Europe developed through a more fragmented and market-driven approach (Russo et al., 2002). Despite these differences, both systems evolved toward increased integration and automation to handle systemic risk and market complexity. From a systems thinking perspective, the paper underscores how exchanges and clearing organizations function as systemic nodes that stabilize the broader financial ecosystem through interconnected risk mutualization and real-time feedback loops. The authors argue that resilience in clearing infrastructure depends on recognizing these interdependencies and embedding adaptive, cross-jurisdictional governance mechanisms.

Despite advancements in traditional risk management, cybersecurity risk management within the broader Enterprise Risk Management (ERM) framework remains fragmented. Traditional risk management methods often treat cybersecurity as an isolated concern, failing to account for its interdependencies with financial, operational, and reputational risks. This siloed approach leaves financial institutions vulnerable to systemic risks, where a single cybersecurity incident can trigger widespread market disruptions.

To address these challenges, this research integrates systems thinking into cybersecurity risk management, offering a holistic and dynamic framework tailored for stock exchanges and clearing organizations. By leveraging systems thinking, this study proposes a comprehensive cybersecurity risk framework that enhances resilience, aligns with regulatory expectations, and improves overall market stability.

The Growing Complexity of Cyber Threats - Cybersecurity risks in financial markets are no longer limited to isolated data breaches; they now encompass advanced

persistent threats (APTs), ransomware attacks, and supply chain vulnerabilities (Dupont, 2019). The increasing sophistication of threat actors, including nation-state cyberwarfare units and organized crime networks, underscores the urgent need for proactive, adaptive cybersecurity strategies. Given the dynamic and evolving nature of cyber threats, financial institutions must move beyond static cybersecurity controls. Instead, they must adopt continuous monitoring, AI-driven threat detection, and predictive analytics to identify and mitigate emerging risks before they materialize (Perlroth, 2021).

1.2 Regulatory Pressures and Compliance Challenges

The U.S. Securities and Exchange Commission (2014) introduced Regulation Systems Compliance and Integrity (Reg SCI) to ensure that key market entities—such as exchanges, clearing agencies, and alternative trading systems—maintain robust technology systems that uphold the stability and integrity of financial markets. Reg SCI mandates regular system testing, incident reporting, and governance protocols to prevent and respond to operational disruptions (U.S. Securities and Exchange Commission, 2014). This regulation institutionalizes systems thinking within market oversight by treating technology infrastructure as a critical subsystem whose failure can propagate systemic risk. Through requirements for continuous monitoring, interdependency mapping, and cross-functional coordination, Reg SCI embeds feedback loops that support adaptive risk management and resilience. It exemplifies how regulatory design can align with systems-based enterprise risk management by fostering organizational learning, transparency, and integrated risk governance.

Stock exchanges and clearing organizations operate in highly regulated environments, where cybersecurity failures can lead to severe financial, reputational, and legal consequences. Regulatory frameworks such as SEC's Reg SCI Compliance, SEC's Cybersecurity Disclosure Guidance, CFTC's Cybersecurity Safeguards (Commodity Futures Trading Commission (CFTC) is a U.S. federal regulatory agency established in 1974. Its primary role is to regulate the U.S. derivatives markets, which include futures, swaps, and certain options markets) and establish stringent cybersecurity requirements for financial institutions. However, regulatory compliance alone is insufficient for cybersecurity resilience. Many financial institutions treat compliance as a box-checking exercise, focusing on meeting minimum regulatory requirements rather than building robust cybersecurity risk management frameworks (Schneier and Miccolis, 1998).

By incorporating systems thinking, financial institutions can move beyond compliance and develop adaptive risk management frameworks that align cybersecurity with business strategy, operational continuity, and financial resilience (Alawattegama, 2018).

The Integration Gap - Cybersecurity and Enterprise Risk Management (ERM). Despite the rise of Enterprise Risk Management (ERM) as a best practice, cybersecurity risks often remain poorly integrated into broader risk management strategies (Taran et al., 2013). Key challenges include, Lack of Integration – Cybersecurity is frequently treated as an independent domain rather than an integral part of enterprise-wide risk assessment. Limited Understanding of Interdependencies – Traditional ERM approaches fail to capture the cascading impact of cyber threats across financial markets. Insufficient Resilience

Measures – While ERM focuses on preventing financial losses, cyber resilience requires rapid response and recovery capabilities. By adopting a systems-thinking approach, financial institutions can map the interdependencies between cybersecurity risks, business objectives, and regulatory requirements (Haywood et al., 2017).

1.3 Applying Systems Thinking to Cybersecurity Risk Management

Abkowitz (2008) demonstrates that catastrophic events seldom arise from a single failure, but instead from interacting technical, human, and cultural factors, echoing systems-thinking's focus on interdependencies. The iterative loop he prescribes—diagnosis, reform, and continuous monitoring—parallels the feedback cycles central to systems thinking and reframes operational risk management as a learning system rather than a compliance exercise (Abkowitz, 2008).

Adopting a systems-thinking approach within enterprise risk management (ERM) provides a transformative framework to better integrate cybersecurity into the core of business operations. The first key step involves identifying business objectives and dependencies, where organizations use systems thinking to visualize the intricate ways cyber risks can impact business operations, financial stability, and regulatory compliance. This process begins by mapping organizational strategic goals to specific business processes, then linking these processes to detailed organizational workflows, and further mapping workflows to the supporting people, processes, and technology systems. This layered mapping enables a comprehensive understanding of operational mechanics and highlights the pathways through which cyber threats can propagate through an organization. Crucially, organizations must also identify key risk drivers such as third-party

vulnerabilities, data breaches, and insider threats, assessing their potential impact on various organizational workflows. Beyond identifying risks, systems thinking emphasizes analyzing the interdependencies between cybersecurity threats and broader operational activities, revealing how disruption in one area can cascade across multiple business functions, amplifying the risk exposure. An essential component of this methodology is the development of feedback loops, where ongoing monitoring and reassessment of the cybersecurity environment allow organizations to refine their strategies continually. These feedback mechanisms integrate real-time risk indicators, threat intelligence, and business process controls, providing an adaptive and resilient framework for identifying, monitoring, and mitigating cybersecurity risks in alignment with the organization's broader risk appetite and operational goals.

Moving from static assessments to dynamic risk management, the second pillar emphasizes enhancing cyber resilience through continuous monitoring. In today's rapidly evolving threat landscape, financial institutions, in particular, must transition from reactive cybersecurity measures to proactive, predictive, and preemptive risk management. Continuous monitoring encompasses several advanced strategies: first, implementing automated threat detection systems that leverage artificial intelligence and machine learning algorithms to identify anomalies within network traffic, application usage, and user behavior, allowing for quicker identification of potential breaches. Second, deploying behavioral analytics tools becomes critical for detecting insider threats and fraudulent activities by monitoring deviations from established user behavior baselines. These tools enable organizations to act swiftly before minor anomalies escalate into major incidents.

Third, scenario-based resilience testing, as emphasized by Bayuk (2024), provides an invaluable technique for simulating cyberattack scenarios and rigorously testing the effectiveness of incident response plans under various stress conditions. Such simulations allow organizations to pinpoint weaknesses in their response protocols and reinforce their defenses accordingly. Continuous monitoring, therefore, not only serves as a protective shield against emerging threats but also fosters a culture of vigilance and adaptability within the institution, enabling it to withstand and quickly recover from potential cyber shocks.

The final element involves aligning cybersecurity initiatives with the overarching business strategy and compliance requirements. Traditional risk management frameworks often treat cybersecurity as a siloed, technical function; however, systems thinking advocates for embedding cybersecurity directly into enterprise-wide risk governance structures. Doing so ensures that cybersecurity considerations are integrated into strategic decision-making processes at the highest organizational levels. A systems-thinking-based alignment yields several tangible benefits. First, it bolsters regulatory compliance by ensuring that cybersecurity practices are consistent with mandates from regulatory bodies such as the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and the Financial Industry Regulatory Authority (FINRA).

Meeting these regulatory expectations not only helps avoid penalties but also ensures that firms are better prepared to navigate the complex regulatory landscape that governs financial markets today. Second, robust cyber risk management practices enhance investor confidence; in an era where cyber incidents can lead to significant reputational and

financial damage, demonstrating a mature cybersecurity posture signals to investors that the organization is well-equipped to manage risks that could otherwise erode shareholder value.

Third, embedding cybersecurity into business strategy improves operational resilience, reducing downtime, safeguarding data integrity, and ensuring business continuity even amidst cyberattacks. This alignment mitigates financial losses, protects critical assets, and enhances customer trust, which is indispensable in maintaining competitive advantage. A prime example is the 2024 CrowdStrike incident, which disrupted multiple industries, including financial institutions reliant on cloud-based security services. Such incidents demonstrate how cybersecurity control operational failures in third-party service providers can cascade across financial markets, affecting liquidity, investor confidence, and regulatory compliance. Systems thinking, therefore, reframes cybersecurity from a cost center to a value-adding component of business strategy, aligning cyber resilience initiatives directly with organizational performance metrics and long-term growth objectives. Through the continuous loop of risk identification, proactive monitoring, and strategic alignment, organizations foster an adaptive risk management culture capable of responding to the unpredictable and increasingly complex cyber threat landscape, ensuring not only compliance and resilience but also sustainable business success.

1.4 Research Objectives and Contributions

This research aims to:

1. Develop a systems-thinking-based cybersecurity risk management approach for stock exchanges and clearing organizations.
2. Provide actionable recommendations for improving regulatory compliance and effective cyber risk management and resilience.

By addressing these objectives, this study contributes to both academic research and industry best practices. It offers a structured methodology for integrating cybersecurity into enterprise risk management, ensuring that financial institutions can navigate an increasingly complex cyber threat landscape. As cyber threats continue to evolve, financial institutions must adopt a proactive, interconnected approach to cybersecurity risk management. Traditional ERM models fail to account for the dynamic nature of cyber risks, leading to compliance gaps, operational inefficiencies, and systemic vulnerabilities (Hoyt and Liebenberg, 2011). By integrating systems thinking into ERM, this research provides a roadmap for financial institutions to enhance cyber resilience, align with regulatory frameworks, and safeguard the integrity of global markets.

1.5 Research Problem

The increasing reliance on digital infrastructure in financial markets has intensified cybersecurity risks for stock exchanges and designated clearing organizations. These institutions play a pivotal role in ensuring market stability, managing transactions, and protecting financial assets (Krueger, 2006). However, the evolving threat landscape,

characterized by state-sponsored attacks, ransomware incidents, and supply chain vulnerabilities, presents unprecedented risks to financial stability (Dupont, 2019).

Despite their critical role, stock exchanges and clearinghouses continue to struggle with integrating cybersecurity into Enterprise Risk Management (ERM) frameworks. Traditional risk management approaches often treat cyber threats in isolation from financial, operational, and reputational risks (Schneier and Miccolis, 1998). This siloed approach results in poor visibility, fragmented governance, and reactive risk mitigation, leaving financial institutions vulnerable to systemic cyber risks.

Additionally, compliance-driven cybersecurity strategies emphasize regulatory adherence over adaptive risk mitigation. Regulations such as the SEC's Cybersecurity Disclosure Guidance and the CFTC's Cybersecurity Safeguards impose stringent cybersecurity requirements on financial institutions. However, these regulations alone do not guarantee cyber resilience, as many organizations prioritize meeting regulatory requirements over building proactive, risk-based security frameworks (Alawattegama, 2018).

This research identifies a gap in cybersecurity risk management: the failure to integrate formal systems thinking into ERM. A systems-thinking approach provides a holistic perspective, mapping interdependencies between cyber risks, business operations, and regulatory mandates, thereby enabling financial institutions to anticipate and mitigate risks dynamically (Haywood et al., 2017).

1.6 Deficiencies in Traditional Cybersecurity Risk Management Approaches

1. Fragmented Risk Management Structures - Financial institutions have traditionally treated cybersecurity as a standalone function, isolated from broader financial and operational risk management frameworks (Hoyt and Liebenberg, 2011). This fragmented structure creates several vulnerabilities that hinder an organization's ability to manage risks effectively. One of the most significant issues arising from this separation is limited risk visibility. When cybersecurity is siloed, organizations often fail to recognize the complex interdependencies between cybersecurity risks and financial stability (Bharathy and McShane, 2014). Cyber threats no longer operate in isolation; an incident such as a data breach or ransomware attack can quickly escalate into broader financial disruptions, undermining operational integrity, eroding customer trust, and incurring regulatory penalties. Without an integrated risk view, institutions are ill-equipped to foresee and prepare for these cascading effects. In addition to limited visibility, the separation fosters reactive cybersecurity strategies. Firms that operate with fragmented structures often prioritize incident response over proactive risk prevention (Siegel et al., 2002). This reactive approach leaves institutions perpetually on the back foot, addressing breaches only after damage has been done rather than implementing robust preventative measures that could thwart threats in their early stages. Reactive strategies also tend to be more resource-intensive and costly over time, as they require significant recovery efforts and can result in prolonged operational downtime. Proactive cybersecurity, in contrast, not only reduces the likelihood of a successful attack but also enhances organizational resilience by fostering a culture of preparedness and continuous improvement. Moreover, fragmented structures

lead to disjointed governance models. When cybersecurity teams and enterprise risk management (ERM) teams function independently, it creates communication gaps, misaligned priorities, and inconsistent risk assessments (Taran et al., 2013). This lack of cohesion weakens the overall governance framework, reducing an institution's ability to coordinate comprehensive responses to complex risk scenarios that span multiple domains. Effective risk management requires seamless collaboration across departments, ensuring that cybersecurity considerations are embedded in financial and operational decision-making processes. Disjointed governance also complicates regulatory compliance efforts, as institutions must demonstrate to regulators that they have holistic risk management frameworks capable of addressing today's multifaceted threat environment. To overcome these challenges, financial institutions must adopt a systems-thinking-based cybersecurity risk model. Systems thinking enables organizations to view cybersecurity as an interconnected component of the overall risk ecosystem, recognizing how threats can propagate across business functions and trigger systemic risks (Ghon Rhee, 2000). By integrating cyber risk into enterprise-wide risk governance structures, institutions can align security investments with business objectives, enhance risk visibility, and improve regulatory compliance. This integrated approach fosters greater organizational resilience by promoting proactive risk identification, mitigation, and response strategies. Furthermore, it ensures that cybersecurity is not merely a technical function but a strategic priority that supports the institution's long-term stability and growth. In an era where cyber threats are becoming increasingly sophisticated and pervasive, adopting a systems-thinking approach

is no longer optional—it is essential for maintaining financial health, operational continuity, and stakeholder confidence.

2. Inadequate Cyber Resilience and Incident Response Strategies - Current cybersecurity strategies in financial institutions predominantly emphasize prevention, concentrating heavily on measures such as firewalls, intrusion detection systems, and endpoint protection. However, despite these efforts, there is a notable deficiency in robust resilience and recovery mechanisms, which leaves institutions vulnerable to increasingly sophisticated cyberattacks that prevention alone cannot fully deter (Schneier and Miccolis, 1998). As threat actors evolve and cyber incidents become more complex and disruptive, the limitations of a prevention-centric strategy become increasingly apparent. Financial institutions must move beyond static defenses and adopt a more dynamic approach that not only aims to prevent breaches but also ensures rapid recovery and minimal disruption when breaches inevitably occur. This shift requires a focus on cyber resilience, a concept that emphasizes an organization's ability to withstand, respond to, and recover from cyber events effectively. Building cyber resilience begins with continuous threat monitoring and real-time anomaly detection (Haywood et al., 2017). Unlike periodic audits or scheduled assessments, continuous monitoring provides ongoing oversight of network activity, allowing for the immediate identification of deviations from baseline behavior. Machine learning and artificial intelligence are often employed to enhance anomaly detection capabilities, enabling organizations to catch subtle indicators of compromise before they escalate into full-scale incidents. Early detection is critical in limiting the scope and impact of attacks, offering valuable lead time to initiate response protocols and prevent

widespread damage. However, detection alone is insufficient without a robust and timely response. Automated incident response frameworks have emerged as a key component of a resilient cybersecurity posture. These frameworks enable organizations to respond to incidents quickly and systematically, minimizing the financial, operational, and reputational fallout associated with cyberattacks (Dupont, 2019). Automation reduces the time it takes to contain breaches and ensures that responses are consistent and repeatable, which is particularly important in high-stress situations where manual intervention can be slow or error-prone. For financial institutions operating in fast-moving markets, delays in response not only jeopardize operational continuity but can also have ripple effects on market stability and investor confidence. Another essential element of cyber resilience is scenario-based risk modeling. By simulating various cyberattack scenarios, financial institutions can anticipate the cascading impacts of different threat vectors across their interconnected systems (Krueger, 2006). Scenario modeling helps organizations understand potential vulnerabilities that may not be apparent during regular operations, enabling them to strengthen their defenses and refine their response strategies. These exercises prepare institutions for a range of possible incidents, ensuring they are not caught off guard when real threats materialize.

Incorporating a systems-thinking approach further amplifies resilience efforts. Systems thinking encourages financial institutions to visualize risk interdependencies and understand the broader cause-and-effect relationships that exist within their organizational structures (Hoyt and Liebenberg, 2011). Rather than viewing cyber risks in isolation, systems thinking promotes a holistic understanding of how vulnerabilities in one area can

propagate throughout the enterprise. This perspective supports the development of adaptive risk mitigation strategies that are better suited to today's complex and rapidly changing cyber threat landscape. By combining continuous monitoring, automated response, scenario-based modeling, and systems thinking, financial institutions can create a resilient cybersecurity framework capable of not only defending against threats but also ensuring swift recovery and sustained operational integrity.

3. Compliance-Driven versus Risk-Based Cybersecurity - Many financial institutions continue to prioritize regulatory compliance over true cybersecurity resilience, focusing primarily on meeting the minimum standards required by governing bodies rather than developing dynamic, forward-looking risk management strategies (Siegel et al., 2002). While compliance is undeniably important for maintaining legal and reputational standing, an overemphasis on regulatory checklists can inadvertently undermine broader cybersecurity objectives. Institutions that view compliance as the ultimate goal often settle for static policies and procedural updates that satisfy auditors but fail to address the rapidly evolving nature of cyber threats. As a result, organizations expose themselves to a false sense of security, believing they are protected when in reality their defenses may be ill-equipped to counter sophisticated, real-world attacks. One major consequence of this compliance-centric mindset is regulatory fragmentation. Financial institutions must navigate a complex web of cybersecurity mandates issued by multiple regulatory agencies at the federal, state, and sometimes international levels. These overlapping regulations often differ in scope, detail, and enforcement expectations, leading to confusion and inefficiency (Taran et al., 2013). Institutions that manage compliance in silos may end up

duplicating efforts or, worse, overlooking critical vulnerabilities that fall outside narrowly defined regulatory requirements. This fragmented approach consumes valuable resources and detracts from the creation of cohesive, enterprise-wide cybersecurity strategies. Another problem is the limited adaptability of static cybersecurity policies. Regulatory standards tend to be reactive, codifying best practices based on past incidents rather than anticipating future threats. Consequently, organizations that build their cybersecurity programs around compliance requirements often find themselves lagging behind the threat landscape (Alawattegama, 2018). Emerging risks—such as ransomware-as-a-service, supply chain attacks, and zero-day vulnerabilities—require adaptive, continuously evolving security strategies. Static policies and infrequent updates make it difficult for institutions to pivot quickly in response to new types of attacks, leaving them vulnerable to highly dynamic threat actors. Furthermore, treating cybersecurity merely as a compliance function weakens its integration with broader business objectives. In many institutions, cybersecurity investments are still perceived primarily as a cost center, justified only to meet legal mandates rather than recognized as strategic enablers of operational resilience and competitive advantage (Ghon Rhee, 2000). This view restricts cybersecurity's role in organizational decision-making processes and inhibits the allocation of sufficient resources toward developing robust, proactive defenses. Without strategic alignment, cybersecurity programs may lack executive buy-in and be underfunded, further diminishing their effectiveness. Systems thinking encourages organizations to view cybersecurity as an interconnected element of their overall risk and governance structures rather than a standalone compliance issue (Hoyt and Liebenberg, 2011). By visualizing

how cyber risks interact with other operational, financial, and reputational risks, institutions can develop proactive, risk-based governance frameworks that enhance resilience. Systems thinking fosters adaptability, allowing organizations to dynamically adjust their cybersecurity strategies as the threat landscape evolves. It also promotes better alignment between cybersecurity initiatives and business objectives, helping institutions to view cyber resilience not as a regulatory burden but as a critical component of their strategic success and long-term stability.

1.7 Purpose of Research

The increasing complexity of financial markets, coupled with the rapid advancement of technology, has led to an escalation of cybersecurity threats targeting stock exchanges and designated clearing organizations. These institutions play a crucial role in ensuring market stability, transaction integrity, and financial security. However, traditional risk management strategies remain largely fragmented and reactive, focusing predominantly on financial and operational risks while failing to integrate cybersecurity threats into a holistic enterprise risk management (ERM) framework. This research seeks to bridge the gap between siloed cybersecurity risk management and enterprise-wide risk governance by applying systems thinking to develop a more dynamic and adaptive cybersecurity risk management framework. The study aims to enhance risk resilience, regulatory compliance, and business continuity within stock exchanges and clearing organizations, ensuring that cybersecurity threats are treated as integral components of the overall risk landscape.

1.8 Research Objectives

1. Integrating Systems Thinking for Cybersecurity Risk Management as part of Enterprise Risk Management - One of the primary objectives of this research is to incorporate systems thinking principles into cybersecurity risk management as part of enterprise risk management within stock exchanges and designated clearing organizations. Systems thinking emphasizes the interconnections and interdependencies between risk factors and critical success factors, helping organizations move beyond siloed risk management structures which primarily becomes a compliance-based approach.

   By integrating systems mapping and feedback loops, this study aims to identify key risk drivers and dependencies within financial institutions and establish cyber risk that align with broader ERM strategies.

2. Bridging the Gap Between Theory and Practical Implementation - While cybersecurity risk management and ERM frameworks have been extensively researched, their integration remains limited in practical applications. This research seeks to develop a framework that translates systems thinking principles into actionable cybersecurity strategies.

1.9 Significance of the Study

The increasing reliance on digital infrastructure in financial markets has made cybersecurity risk management a critical concern for stock exchanges and designated clearing organizations. These institutions ensure market stability, facilitate transactions, and safeguard financial assets, yet they remain prime targets for cyber threats. Traditional

Enterprise Risk Management (ERM) frameworks often fail to integrate cybersecurity risks effectively, leaving financial institutions vulnerable to systemic disruptions. Traditional risk management models often treat risks in isolation, neglecting the interdependencies between cybersecurity, operational, and financial risks. For example, traditional ERM frameworks such as COSO ERM and ISO 27001 provide structured approaches to risk identification and assessment but fail to integrate cybersecurity risk into enterprise-wide decision-making which can also have a material business impact.

This research addresses a pressing gap in cybersecurity risk management by integrating systems thinking into ERM. By applying this holistic approach, the study aims to enhance cyber resilience, improve regulatory compliance, and strengthen decision-making within financial institutions.

1. Financial institutions continue to be prime targets for cyberattacks, as threats such as supply chain vulnerabilities, insider risks, and ransomware incidents grow increasingly sophisticated and prevalent. Traditional, siloed approaches to cybersecurity are no longer sufficient to combat the evolving threat landscape. In response, applying systems thinking provides a more holistic framework to strengthen cyber resilience across the financial sector. Systems thinking ensures that cybersecurity measures are not treated as isolated technical controls but are embedded deeply into broader enterprise risk management (ERM) strategies. By integrating cybersecurity within ERM, organizations can ensure that cyber risks are evaluated and managed alongside financial, operational, and reputational risks, creating a unified and more resilient risk posture. Additionally, a systems-thinking approach enhances the risk assessment framework, helping financial institutions gain a

clearer understanding of how cyber incidents can directly impact business objectives, operations, and financial stability. This integrated perspective allows organizations to move beyond generic threat identification and toward more targeted risk mitigation strategies that prioritize business continuity. Furthermore, systems thinking promotes the adoption of continuous monitoring and real-time cyber risk intelligence, enabling institutions to detect, assess, and respond to threats as they emerge. Continuous monitoring provides the visibility needed to spot anomalies early, while real-time intelligence ensures that risk management strategies evolve in step with the dynamic cyber threat environment. Together, these elements foster a proactive and adaptive cybersecurity posture, better positioning financial institutions to withstand and recover from increasingly complex and damaging cyberattacks.

2. Strengthening regulatory compliance and governance has become increasingly important as regulatory agencies such as the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) emphasize the critical role of cyber risk governance in financial institutions. Despite these regulatory pressures, many firms continue to approach cybersecurity in a reactive manner, focusing on fulfilling minimum compliance requirements rather than adopting cybersecurity as a strategic imperative. This reactive stance limits their ability to anticipate and effectively manage evolving threats, resulting in fragmented governance models that fail to integrate cybersecurity into broader enterprise risk management frameworks. To address this gap, this study aims to provide a comprehensive framework for integrating cybersecurity risk management directly into governance structures. By embedding cyber risk considerations

into board-level oversight and strategic decision-making processes, financial institutions can move beyond checkbox compliance and foster a culture of proactive cyber resilience. Such integration ensures that cybersecurity is treated not merely as a regulatory requirement but as a fundamental component of corporate governance, aligning security initiatives with organizational objectives and regulatory expectations. The proposed framework will guide institutions in designing governance models that promote accountability, enhance risk visibility, and enable timely responses to the increasingly complex cyber threat landscape.

3. Improving decision-making through systems thinking has become essential as traditional risk management frameworks increasingly show their limitations in dealing with the complexity of cyber threats. These traditional models often view risks in isolation, failing to account for the interconnected and dynamic nature of cyber risks across various business processes and technological systems. This lack of integration leads to poor risk visibility and ineffective response strategies, leaving financial institutions vulnerable to threats that can quickly cascade across departments and functions. By adopting a systems-thinking approach, financial institutions can enhance their strategic decision-making processes by conducting more sophisticated risk analyses that recognize and account for these interdependencies. Systems thinking enables organizations to map out how a cyber event in one part of the business could impact other critical operations, providing leaders with clearer insights into potential vulnerabilities and systemic weaknesses. Furthermore, this approach supports the development of more comprehensive, risk-based control designs and implementation strategies that are tailored to the interconnected realities of today's

operational environments. Rather than applying generic cybersecurity controls, institutions can design targeted measures that specifically address the pathways through which cyber risks propagate, strengthening their overall defense posture. Ultimately, systems thinking shifts the focus from reactive incident management to proactive, informed decision-making, enabling financial institutions to better protect themselves against the increasingly sophisticated and interconnected cyber threats they face.

Bridging the gap between academia and industry practices is a critical objective of this research, aiming to ensure that theoretical advancements are directly applicable to real-world challenges. While academic research often provides valuable frameworks and models, there can be a disconnect when these theories are not easily translated into industry practices. This study seeks to close that gap by providing a practical framework specifically designed for implementation within stock exchanges, clearing organizations, and other financial market infrastructures. The framework will not only be grounded in rigorous academic principles but also tailored to the operational realities and regulatory environments that these institutions navigate daily. By incorporating insights and feedback from industry practitioners, the research ensures that its recommendations are both practical and actionable, addressing the nuanced challenges that professionals face in managing cybersecurity risks. Real-world perspectives enhance the relevance of the findings, offering financial institutions strategies that are tested against actual industry needs rather than purely theoretical constructs. Ultimately, this dual focus on academic rigor and practical application aims to enrich both scholarly understanding and industry best practices, fostering stronger collaboration between the two spheres and advancing

cybersecurity resilience across financial market infrastructures.

1.10 Research Purpose and Questions (RQ)

1. RQ1 - How can systems thinking be applied to cybersecurity risk management within the Enterprise Risk Management (ERM) framework of stock exchanges and clearing houses?
2. RQ2 - What governance models can be adopted for cybersecurity risk governance as part of enterprise risk management?

CHAPTER II:

2. REVIEW OF LITERATURE

2.1 Evolution of Financial Market Infrastructures and Securities Regulation

The evolution of securities exchanges in the United States represents a significant case of structural transformation in financial markets. Dombalagian (2020) details how traditional exchanges once operated as mutual organizations owned by brokers and dealers. This alignment of participant interests was central to their cooperative nature. With demutualization, exchanges transitioned into for-profit entities with public shareholders, a shift that has led to new governance models and raised regulatory issues regarding the balance between profit motives and market integrity (Aggarwal et al. 2007).

Krueger (2006) contributes to this understanding by tracking the evolution of clearing and settlement processes. Notably, the shortening of settlement cycles—from T+5 in earlier decades to T+3 and even discussions of T+1 today—reflects the market's adaptation to increasing trade volumes and technological advancements. Milne (2007) emphasizes the importance of network externalities and economies of scale in the post-trade clearing and settlement industry, which has facilitated a consolidation of service providers even as global competition intensifies.

Technological advances have played a key role in reshaping market infrastructure. Innerhofer-Oberperfler and Breu (2006) illustrate how enterprise architecture can be employed to streamline trade processing and risk management. Concurrently, new technologies such as blockchain and distributed ledger technology (DLT) are emerging as potential platforms for further modernizing clearing and settlement systems (Milne, 2007).

Globalization has compounded these challenges. Aggarwal et al. (2007) discuss how U.S. securities regulation is increasingly pressured by the dynamics of global exchanges. Firms are frequently caught between stringent domestic regulations and the allure of more flexible, internationally oriented platforms. This international tension underlines the need for regulatory harmonization that takes into account global competitive dynamics.

As financial infrastructures evolve, regulatory bodies have had to adapt. Rabinowitz (2020) highlights the expanding role of the SEC in overseeing not only traditional financial disclosures but also cybersecurity aspects that impact market stability. Trautman and Newman (2022) propose the creation of a Cyber Data Disclosure Advisory Commission to standardize how cyber incidents are reported, ensuring consistency and transparency. These proposed regulatory enhancements are essential to balancing market efficiency with investor protection. Aebi et al. (2012) further observe that effective risk management and corporate governance during crises—particularly in banking—can be decisive in maintaining market stability. They find that banks where the Chief Risk Officer (CRO) reports directly to the board tend to perform better, suggesting that robust internal oversight is critical during periods of market stress.

2.2 Cybersecurity and Cyber-Resilience in Financial Systems

Traditionally, cybersecurity was driven by the "prevent and protect" mindset. Dupont (2019) argues that this paradigm is increasingly inadequate given the sophistication and inevitability of cyberattacks. Instead, organizations are now emphasizing cyber-resilience—defined as the ability to absorb, recover, and adapt to attacks. Gottipati (2020) extends this discussion by proposing a cybersecurity model for cryptocurrency exchanges

that incorporates real-time application self-protection (RASP), hardware security modules (HSM), and a comprehensive incident response plan. Johnson (2015) furthers the discussion by illustrating how conventional regulatory measures often lag behind emerging cyber threats, leaving financial institutions vulnerable. This critique resonates across the literature, as cyber-resilience models not only protect data but also provide a framework for recovery and adaptation in the event of an attack.

Numerous empirical studies have quantified the adverse effects of cyber-attacks on firm value and market performance. Arcuri et al. (2018) find that announcements of cyber-attacks lead to significant negative abnormal returns, especially in sectors where trust is paramount. Similarly, Gordon et al. (2011) document a downward shift in stock returns following security breaches, noting that breaches affecting system availability have particularly severe effects. Jimmy (2024) demonstrates that beyond immediate price drops, cyber-attacks can result in long-term market instability, increased costs for enhanced security measures, and even regulatory fines. Kammoun et al. (2019) provide further granularity by showing that the timing of disclosure—from the incident to the public announcement—plays a crucial role in determining the market reaction. These studies collectively emphasize that the costs associated with cyber breaches extend well beyond the immediate technical damage, impacting investor confidence and firm valuation over the long haul.

Disclosures related to cyber breaches have become increasingly important. Deane et al. (2019) show that information security certification announcements can have positive market effects, suggesting that transparency and accountability can mitigate negative

impacts. However, Gordon et al. (2024) and Trautman and Newman (2022) both note that current disclosure practices are often vague and inconsistent. In many cases, companies issue 8-K filings that do not provide sufficient detail on the material impact of an incident. Rabinowitz (2020) argues that to build investor trust and market stability, regulatory bodies such as the SEC must expand their oversight to encompass detailed cybersecurity disclosures. This call is echoed by Romanosky and Petrun Sayers (2021), who report that many organizations treat cyber risk as an operational concern rather than embedding it into their broader ERM frameworks. Clear, standardized guidelines for cyber incident reporting are crucial to ensuring that stakeholders receive the information they need to make informed decisions.

The integration of cyber risk into ERM frameworks has become a focal point in contemporary risk management literature. Althonayan and Andronache (2019) argue that aligning cybersecurity with ERM enables organizations to adopt a strategic foresight approach that incorporates scenario planning and predictive analytics. This integration ensures that cyber risks are addressed not only as isolated IT issues but as systemic threats that can impact the entire enterprise.

Lee (2021) presents a four-layer Cyber Risk Management Framework that includes components for assessing the external cyber ecosystem, safeguarding internal infrastructures, conducting rigorous risk assessments, and continuously monitoring performance. By adopting such a multi-layered approach, organizations can allocate resources more effectively and ensure that their cybersecurity investments translate into long-term resilience. Al-Alawi and Al-Bassam (2020) also contribute to this discussion by

highlighting the significance of comprehensive cybersecurity systems in managing risk in the banking and financial sectors. They underscore the necessity of cultivating cybersecurity awareness among employees and ensuring that top management allocates sufficient resources to these initiatives. In this way, organizations can not only protect against immediate cyber threats but also foster a culture of resilience that anticipates future challenges.

2.3 Enterprise Risk Management (ERM): Evolution and Strategic Integration

Traditional risk management practices have often been compartmentalized, focusing on isolated risks without considering the wider operational, strategic, and external contexts. Al-Khadash, Jireis, and Embassy-Jordan (2017) survey all thirteen Jordanian commercial banks and compile a composite score for each COSO ERM component, then regress those scores against profitability metrics, finding that fuller ERM implementation significantly lifts Return on Assets (ROA) and Return on Equity (ROE) after controls for size and leverage. Stoll (2015) explains that this reductionist approach fails to capture the interdependencies that exist in complex organizations. As a result, the evolution toward integrated ERM frameworks, which encompass risk identification, assessment, and mitigation across the entire enterprise, marks a significant shift in strategy. Beasley et al. (2005) surveyed U.S. publicly traded firms and found that ERM implementation depth rises sharply when boards explicitly charge a chief risk officer with coordinating risk information across units, underscoring the need for system-wide oversight rather than siloed control. Larger firms and those with more independent directors also report broader ERM adoption, suggesting that complex organizational “systems” and diverse governance

perspectives foster a holistic, interconnected view of risk. Haywood et al. (2017) and O'Donnell (2005) both articulate how a systems-based view enables organizations to identify cascading risks and preemptively manage them.

Lundqvist (2014) supports this shift by highlighting the four pillars of ERM—risk governance, risk culture, risk quantification, and risk integration into decision-making. Empirical work by Hoyt and Liebenberg (2011) further validates that firms adopting ERM frameworks demonstrate improved market valuations, suggesting that a comprehensive approach to risk management can enhance overall firm performance. Sax and Andersen (2019) emphasize that effective risk management should be closely aligned with an organization's strategic objectives. This integration ensures that risk management is not merely a compliance function but a strategic enabler. Hoyt and Liebenberg (2011) provide evidence that companies with robust ERM practices display higher Tobin's Q ratios—an indicator of market value—implying that stakeholders view strategic risk management favorably. Corporate governance plays a pivotal role in this integration. Aebi et al. (2012) and Malik et al. (2020) stress that the role of the risk committee and the position of the CRO within the organization are essential for ensuring that risk management practices are embedded in the strategic fabric of the firm. Agarwal and Kallapur (2018) further note that a cognitive risk culture, where advanced roles in risk governance are embraced, strengthens an organization's ability to identify and mitigate complex risks. Beasley et al. (2023) add that an ecosystem approach to risk governance, which involves both internal and external stakeholders, enhances the adaptability and effectiveness of risk management processes.

The need to quantify risk has led to the development of various models designed to estimate both inherent and residual risk. Agustina and Baroroh (2016) propose that enhanced financial performance mediates the relationship between ERM and firm value, thereby quantitatively linking risk management with market performance. Kountur (2018) introduces a predictive model where the likelihood of residual risk is a function of the initial risk likelihood, quality of risk treatment, and the appropriateness of the controls implemented. These quantitative approaches provide a more objective basis for prioritizing risk mitigation efforts and optimizing resource allocation. Mathrani and Mathrani (2013) illustrate how enterprise systems can facilitate the conversion of raw data into actionable insights, thereby enhancing risk identification and assessment processes. Similarly, Bromiley et al. (2015) highlight that while ERM frameworks differ in their implementation, organizations that effectively measure risk tend to outperform those that employ a more fragmented approach.

Despite these advances, several critiques have emerged regarding current ERM models. Williamson (2007) and Kurniawanti (2010) argue that frameworks such as COSO ERM have inherent limitations. For instance, COSO's narrow definition of risk and its prescriptive approach may hinder organizations' ability to adapt in dynamic environments. Stoll (2015) also notes that many ERM frameworks suffer from a "check-box" mentality, where compliance takes precedence over strategic risk management. Taran et al. (2013) further critique that ERM, when not integrated into business model innovation, fails to address the inherent uncertainty of the innovation process. These criticisms underscore the need for more flexible, context-specific, and strategically oriented risk management

frameworks that can evolve as organizational and market conditions change. Moşteanu (2020) examines how digitalization and cybersecurity challenges necessitate organizational restructuring, suggesting that traditional hierarchical models may be ill-suited for contemporary risk landscapes. In response, scholars and practitioners alike are advocating for ERM frameworks that are not static but adapt dynamically to internal and external pressures. Acharyya and Brady (2014) argue that ERM education must move beyond siloed, actuarial-style courses and train students to view risks as an interconnected portfolio that spans strategy, finance, operations, and culture. Their pilot curriculum operationalizes systems-thinking by requiring learners to map feedback loops between strategic objectives and risk events, trace cascading consequences across functions, and evaluate control effectiveness in dynamic scenarios. By weaving together ISO 31000, COSO ERM, quantitative analytics, and board-level governance into a single sequence, the program mirrors the holistic architecture that systems-based ERM demands (Acharyya and Brady, 2014).

2.4 Systems Thinking and Its Application in Risk Management

Systems thinking provides a holistic lens through which the complex interrelationships among various risk factors can be understood. White (1995) argues that traditional risk management approaches are often reductionist, failing to capture the nuances of interconnected systems. Stave and Hopper (2007) propose a taxonomy for systems thinking that ranges from recognizing interconnections between components to developing full-scale simulation models that predict behavior under different scenarios.

These theoretical frameworks highlight that understanding feedback loops and emergent properties is crucial for effective risk management.

Salim (2014) uses a systems theory approach to advocate for a comprehensive view of cybersecurity risks. He explains how feedback loops—both positive and negative—can either exacerbate or mitigate risk, suggesting that continuous monitoring is essential for dynamic risk management. O'Donnell (2005) applies systems thinking specifically to the event identification phase in ERM, arguing that mapping the value chain can reveal hidden vulnerabilities that traditional methods might overlook.

A key benefit of applying systems thinking is the ability to use modeling and simulation to predict risk outcomes. Collins (2024) performs a systems literature review that indicates a lack of consistent definitions for "systems thinking" within cybersecurity research, suggesting that future work should focus on standardizing these definitions and methodologies. Sion et al. (2018) describe an approach that integrates risk analysis into threat modeling using Data Flow Diagrams (DFDs) and Monte Carlo simulations. This methodology allows for a probabilistic evaluation of risks and supports the identification of high-risk areas even in complex systems.

Shaked et al. (2020) further argue that embedding systems thinking into a cyber resilience maturity model can probe sectoral design spaces and identify cross-domain vulnerabilities. These simulation approaches enable organizations to run "what-if" scenarios, thereby developing adaptive responses to potential cascading failures. The integration of systems thinking into risk management is not solely a technical exercise—it also requires an adaptive organizational culture. O'Donnell (2005) underscores that a

systems-based approach to risk identification, one that takes into account value chain interdependencies, is only effective if the organization fosters a culture of continuous learning. Spafford et al. (2023) also challenge common cybersecurity myths, arguing that debunking misconceptions is critical to designing more effective, adaptive security systems that account for human factors. This cultural shift towards embracing a holistic view of risk is essential for integrating technological solutions with organizational strategies. Bell et al. (2002) recast external auditing as a "strategic-systems" exercise in which auditors begin by modelling the client's entire business system—strategy, processes, information flows, and external environment—before drilling into account balances. By treating the audit entity as a complex, adaptive system, they stress that risks of material misstatement are best understood through the feedback loops linking strategic objectives to operational performance. Lee and Green (2015) provide a foundational exploration of how systems thinking can reshape enterprise risk management (ERM) by encouraging organizations to shift from linear, siloed risk assessments to holistic, feedback-driven models. They argue that traditional ERM frameworks often fail to capture the complexity of risk interactions across departments, leading to blind spots in strategy execution. Using systems dynamics modeling, they illustrate how reinforcing and balancing feedback loops influence risk emergence and mitigation across organizational subsystems. Their findings suggest that applying systems thinking enhances an organization's capacity for anticipatory learning, adaptive control, and strategic resilience (Lee and Green, 2015). Ultimately, the paper positions systems thinking as a critical lens for transforming ERM into a proactive, integrated process that aligns with complex enterprise environments.

2.5 IT Risk Management and Comparative Frameworks

Enterprise Architecture (EA) is increasingly recognized as a foundational tool for IT risk management. Innerhofer-Oberperfler and Breu (2006) advocate for a model-driven approach whereby EA is used to develop layered representations of an organization—from the business layer to the physical layer. This methodology facilitates the identification of dependencies and potential risk propagation paths that might otherwise remain hidden. Azizi and Hashim (2008) similarly emphasize that a structured categorization of IT risks—ranging from infrastructure development to software and outsourcing risks—enables organizations to systematically address vulnerabilities.

Significant research has compared leading ERM frameworks, notably COSO ERM and ISO 31000. Gjerdrum and Peter (2011) provide a detailed analysis of these frameworks, noting that while COSO was developed with a focus on financial controls and compliance, ISO 31000 offers a more streamlined, process-oriented approach. Critics such as Kurniawanti (2010) argue that the COSO framework's universal assumptions and complex structure can be prohibitive for some organizations, particularly those with limited resources. A core risk-representation model maps causal dependencies among events, explicitly capturing interconnectivity and strategic-context alignment—an approach that mirrors systems-thinking's emphasis on feedback loops and leverage points (Bensaada and Taghezout, 2019). By visualizing how hazards propagate through intertwined processes, the model helps managers prioritize controls and allocate scarce resources where they mitigate systemic vulnerabilities most effectively (Bensaada and Taghezout, 2019). Overall, the study illustrates how a lightweight, modular architecture can embed holistic

systems concepts into SME ERM practice, fostering continuous learning and resilience across the enterprise (Bensaada and Taghezout, 2019).

Williamson (2007) further critiques COSO's static nature and its narrow risk definitions, suggesting that these limitations may undermine its effectiveness in dynamic environments. Together, these studies underscore the need for adaptable, context-specific risk management solutions that draw on the strengths of both frameworks. Quantitative risk models have advanced significantly over recent years. Kountur (2018) presents a predictive model that estimates residual risk likelihood by combining the likelihood of risk before treatment, the quality of the risk treatment, and the appropriateness of the controls. This model offers a way to quantify the residual risk left after mitigation measures have been applied, supporting more informed decision-making. Mathrani and Mathrani (2013) highlight the role of enterprise systems in converting data into actionable insights, thereby enhancing quantitative risk assessments. Bromiley et al. (2015) add that although ERM frameworks vary in their implementation, organizations that incorporate rigorous quantitative measures often experience improved financial performance.

2.6 Integrating Cyber Risk into Broader ERM Frameworks

Cyber risk has traditionally been treated as a specialized IT problem. However, as cyber threats increasingly disrupt business operations and impact market confidence, their integration into broader ERM frameworks has become imperative. Romanosky and Petrun Sayers (2021) note that many organizations continue to classify cyber risk as an operational rather than a strategic issue. Althonayan and Andronache (2019) argue for a strategic foresight approach in which cybersecurity management is aligned with ERM, ensuring that

emerging threats are considered in the overall risk appetite and planning processes. This integration enables organizations to systematically address risks that have both immediate technical implications and longer-term strategic consequences. Lee (2021) introduces a layered Cyber Risk Management Framework that explicitly integrates risk assessment with infrastructure protection and performance monitoring. Such frameworks provide decision-makers with a comprehensive toolset to evaluate cyber risks alongside other enterprise risks, thereby streamlining the prioritization of risk mitigation investments.

Chmielecki et al. (2014) recast cybersecurity as an enterprise-wide, adaptive process that must be governed at the same strategic level as the business functions it supports, rather than relegated to a narrow IT concern. Their "enterprise-oriented" model anchors risk assessment, control selection, deployment, and continuous monitoring in a shared enterprise-architecture blueprint, ensuring that business managers and technologists jointly analyses cascading, escalating, and common-cause failures across business, application, data, and technology layers. By embedding established frameworks—TOGAF, COBIT, ISO 27002, and NIST 800-53—within a Plan-Do-Check-Adjust cycle, the authors create feedback loops that let organizations trace vulnerabilities to strategic objectives and iteratively refine controls as conditions change. Cholez and Feltus (2014) advocate for a systemic approach to risk management that departs from traditional linear and static models by emphasizing the dynamic interrelations among organizational assets, roles, and processes. Their model integrates goal-oriented risk modeling with responsibility alignment, ensuring that risk identification and mitigation are not isolated activities but are embedded in the organization's functional architecture. The proposed approach relies on

continuous feedback loops between operational actors and governance layers, aligning with systems thinking principles that view organizations as complex, adaptive systems. By capturing emergent risks through role-process interdependencies and scenario simulation, their model enables organizations to anticipate vulnerabilities that might otherwise remain hidden in siloed frameworks.

Naudet et al. (2016) also propose a systemic approach for information security risk management that takes into account the interconnected nature of business ecosystems, emphasizing that risks often transcend organizational boundaries. These methodologies point to the necessity of adopting both quantitative and qualitative measures to capture the full spectrum of cyber risk impacts. Al-Alawi and Al-Bassam (2020) further reinforce the importance of integrating cyber risk within the broader ERM context, particularly in sectors like banking and finance, where digitalization has exponentially increased exposure to cyber threats. By ensuring that cyber risk is not isolated but assessed in the context of overall business risk, organizations can build more resilient systems capable of withstanding both operational and strategic shocks. M'manga (2020) explores how cybersecurity decision-making can be enhanced through risk-based design principles that integrate technical controls with organizational context and human factors. The research presents a framework that combines threat modeling, stakeholder engagement, and contextual risk visualization to support informed, enterprise-wide cybersecurity governance. Central to the model is the recognition that cybersecurity decisions are influenced by feedback from dynamic risk environments, aligning with systems thinking's emphasis on interconnectedness and adaptive learning. The study advocates for embedding

cybersecurity into broader risk management frameworks through iterative loops of monitoring, evaluation, and redesign. This approach enables organizations to move beyond reactive compliance and toward proactive, risk-informed cybersecurity strategies that are responsive to systemic vulnerabilities. Oosthoek and Doerr (2020) analyze cybersecurity threats targeting Bitcoin exchanges, focusing on how adversaries exploit systemic weaknesses and laundering pathways. Their study identifies patterns such as credential stuffing, social engineering, and cross-platform laundering schemes, demonstrating how attackers navigate complex, interconnected systems to bypass traditional controls (Oosthoek and Doerr, 2020). By mapping exploitation techniques across multiple attack surfaces—including APIs, user interfaces, and financial networks—the authors reveal the systemic nature of exchange vulnerabilities. Their findings highlight the need for dynamic, feedback-oriented cybersecurity risk management that adapts to emerging threat ecosystems. This aligns with systems thinking by recognizing that securing decentralized financial platforms requires monitoring interactions across technology, human behavior, and institutional structures.

2.7 Financial Impacts, Residual Risk, and Disclosure Practices

The U.S. Securities and Exchange Commission (2023) introduced the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rule (Release No. 33-11216) to enhance transparency and accountability in how public companies manage cyber risks. The rule mandates timely disclosure of material cybersecurity incidents via Form 8-K and requires detailed annual reporting on governance structures, risk oversight processes, and board involvement in cybersecurity strategy (U.S. Securities and Exchange

Commission, 2023). This regulation operationalizes systems thinking by institutionalizing feedback mechanisms that link operational cybersecurity controls with executive oversight and market-facing disclosures. It reinforces the notion that cybersecurity is not an isolated IT issue but a strategic enterprise-wide concern that influences investor confidence and systemic market stability. The rule promotes continuous risk monitoring and adaptive governance, aligning with systems-based enterprise risk management principles (U.S. Securities and Exchange Commission, 2023). The U.S. Securities and Exchange Commission (2023) requires public companies to file Form 10-K annually under the Securities Exchange Act of 1934, providing a comprehensive overview of financial performance, material risks, and governance practices. Increasingly, this includes detailed cybersecurity risk disclosures, reflecting the growing recognition that cyber threats are material to firm value and stakeholder confidence (U.S. Securities and Exchange Commission, 2023). These disclosures create transparency across investor, regulatory, and internal oversight channels—key feedback loops in a systems-thinking approach to enterprise risk management. By institutionalizing structured, periodic reflection on cyber and operational risk exposure, Form 10-K reinforces the role of continuous learning and governance alignment in maintaining organizational resilience (U.S. Securities and Exchange Commission, 2023).

Empirical research has documented that cyber-attacks can have significant adverse effects on firm performance and market value. Arcuri et al. (2018) note that cyber-attack announcements result in negative abnormal returns, especially in industries where consumer trust and data confidentiality are critical. Gordon et al. (2011) confirm that

security breaches lead to noticeable declines in stock prices. Additionally, research by Kammoun et al. (2019) reveals that while immediate market reactions are negative, there is sometimes a rebound in stock prices after financial losses become fully recognized. Jimmy (2024) outlines how the ripple effects of cyber-attacks can persist over the long term, contributing to sustained market volatility and increased costs in cybersecurity investments.

The quantification of residual risk—the risk that remains after mitigation measures are applied—has become an important aspect of contemporary risk management. Kountur (2018) offers a model that predicts the likelihood of residual risk, providing key insights into how risk treatment quality and appropriateness can be measured. This quantitative approach is essential for developing risk maps and determining the efficiency of risk mitigation strategies. Such models, when integrated with enterprise systems, can transform qualitative data into meaningful quantitative metrics that support strategic decision-making.

Gordon et al. (2024) present exploratory empirical evidence on how U.S. public firms disclose cybersecurity breaches, highlighting significant inconsistencies in disclosure timing, language, and content. Their findings suggest that, despite regulatory expectations for transparency, many firms delay or underreport breach details, often framing disclosures in vague or non-technical terms. This fragmented reporting behavior undermines stakeholders' ability to assess cyber risk exposure accurately, pointing to systemic gaps in governance and communication. From a systems-thinking perspective, the study underscores how weak feedback mechanisms between incident detection, executive oversight, and market disclosure can distort the risk signal and impair organizational learning. Integrating real-time, structured cyber event reporting into enterprise risk

management could strengthen transparency, accountability, and adaptive governance. The transparency of cyber risk information is crucial for both investor confidence and regulatory compliance. Deane et al. (2019) note that positive market responses can be associated with detailed and transparent information security disclosures. This initiative is supported by Rabinowitz (2020), who argues that enhanced disclosure guidelines will help mitigate the negative market impact by providing stakeholders with more accurate and actionable information about cyber incidents. Smith et al. (2019) analyze the financial repercussions of cybercrime on publicly traded companies, revealing a statistically significant decline in stock prices following the disclosure of cyber incidents. Their study emphasizes that investor reactions are shaped not just by the breach itself but also by the perceived adequacy of the firm's response and risk governance practices. This finding highlights the systemic nature of cyber risk, where technical failures trigger cascading impacts across reputation, market valuation, and regulatory scrutiny. From a systems thinking perspective, the study underscores the importance of feedback loops between cybersecurity readiness, public perception, and financial outcomes. Effective enterprise risk management must therefore incorporate not only preventive controls but also crisis communication and strategic transparency to manage the broader system-level consequences of cybercrime (Smith et al., 2019).

2.8 Organizational Dynamics, Culture, and the Future of Risk Governance

An organization's culture and governance structure are critical determinants of its ability to manage risk holistically. Agarwal and Kallapur (2018) highlight that a cognitive risk culture—one that fosters advanced roles in risk governance—is essential for proactive

risk management. Beasley et al. (2023) further assert that risk governance functions as an ecosystem, where both internal and external forces shape risk management strategies. These perspectives imply that effective ERM requires strong leadership, clear accountability structures, and a culture that promotes openness and adaptability.

Stoll (2015) adds that transitioning from information security management to enterprise-wide risk management involves a significant cultural shift—one that must integrate stakeholder requirements and regulatory demands into the day-to-day functioning of the organization. Moşteanu (2020) examines the challenges posed by digitalization and cybersecurity in necessitating organizational restructuring, arguing that firms must develop integrated approaches to address the evolving risk landscape. These insights underscore that the future of risk governance will depend on an organization's ability to foster a resilient and adaptive culture. Arena et al. (2010) propose that ERM is a dynamic process that evolves alongside organizational changes. Their research suggests that effective risk governance requires continuous feedback between risk identification, risk management practices, and organizational learning. Similarly, Beasley et al. (2023) describe risk governance as an ecosystem—a network of activities and actors that collectively contribute to the organization's risk posture. Bromiley et al. (2015) argue that such an ecosystem approach, which encompasses both quantitative and qualitative dimensions of risk, can lead to more informed strategic decision-making. Furthermore, Spafford et al. (2023) challenge conventional cybersecurity myths and call for a more nuanced understanding of risk that considers both human behavior and technical measures. Their work, together with O'Donnell's (2005) systems-thinking framework, suggests that visualizing risk in the form

of process models or heat maps is essential to capture the complexity of interdependent risk events. This approach promotes a more proactive and adaptive management style that is critical in today's fast-changing risk environments.

Current research into ERM and cybersecurity reveals several directions for future inquiry. Collins (2024) calls for a unified definition of systems thinking within cybersecurity contexts to standardize methodologies. Salim (2014) and O'Donnell (2005) emphasize the need for dynamic models that can adapt to rapidly changing risk landscapes. Moreover, Trautman and Newman (2022) and Rabinowitz (2020) advocate for regulatory innovation, including the establishment of advisory bodies to standardize disclosure practices and improve transparency. Bromiley et al. (2015) and Arena et al. (2010) both note that while significant progress has been made in integrating risk management into organizational strategy, challenges remain in measuring the tangible benefits of such integration. As such, further empirical research is needed to refine measurement techniques, validate predictive models for residual risk, and ensure that risk management processes remain agile and context-sensitive. Mathrani and Mathrani (2013) also highlight the role of enterprise systems in transforming raw risk data into actionable intelligence. With the advent of advanced analytics and big data technologies, future research is likely to focus on how these tools can further improve risk quantification and enhance decision-making at both operational and strategic levels.

The transformation of securities exchanges from mutual organizations to demutualized, publicly traded entities (Dombalagian, 2020; Aggarwal et al., 2007) underscores how technological innovation and globalization have reshaped market

dynamics. Concurrently, the paradigm shifts in cybersecurity—from prevention to resilience—is critical as organizations face increasingly sophisticated cyber threats (Dupont, 2019; Gottipati, 2020; Johnson, 2015). Integrated ERM frameworks have emerged as essential for bridging the gap between isolated risk management practices and the complex realities of modern business. Empirical studies consistently show that firms with robust ERM—and particularly those that integrate cybersecurity risk—tend to enjoy greater market stability and improved financial performance (Hoyt and Liebenberg, 2011; Lundqvist, 2014; Malik et al., 2020; Romanosky and Petrun Sayers, 2021). At the same time, critics of existing frameworks, such as COSO ERM, advocate for more flexible and adaptive approaches that account for dynamic risk environments (Kurniawanti, 2010; Williamson, 2007; Stoll, 2015).

A systems thinking approach emerges as a common thread throughout the literature. By emphasizing interdependencies, feedback loops, and dynamic modeling, systems thinking provides both a theoretical and practical foundation for modern risk management (White, 1995; Salim, 2014; O'Donnell, 2005; Stave and Hopper, 2007). Quantitative models for residual risk estimation further support this integrated approach, enabling organizations to translate qualitative insights into strategic actions (Kountur, 2018; Mathrani and Mathrani, 2013). Moreover, the integration of cyber risk into broader ERM frameworks is now recognized as indispensable—not only for protecting digital assets but also for maintaining investor confidence and ensuring regulatory compliance (Al-Alawi and Al-Bassam, 2020; Althonayan and Andronache, 2019; Lee, 2021). Future research, as suggested by Collins (2024) and Trautman and Newman (2022), should focus on

standardizing definitions and disclosure practices, integrating cutting-edge analytic tools, and further validating the economic benefits of holistic risk management.

Organizational dynamics, including governance, culture, and leadership, also play a critical role. Studies by Agarwal and Kallapur (2018), Arena et al. (2010), and Beasley et al. (2023) highlight how a risk-aware culture, supported by robust governance structures, is essential to harnessing the full benefits of ERM. The push toward standardization of cybersecurity disclosures and the incorporation of real-time monitoring systems reflects the broader trend toward greater transparency and accountability in risk management (Deane et al., 2019; Gordon et al., 2024; Rabinowitz, 2020). Ultimately, the literature paints a picture of a rapidly evolving landscape where risk management must be both integrated and dynamic. The fusion of traditional financial oversight with modern cybersecurity, ERM, and systems thinking represents not only an academic achievement but also a practical necessity for organizations operating in today's uncertain global environment. As digital transformation accelerates and new threats emerge, the continuous evolution of risk management practices will remain central to sustaining market integrity and ensuring organizational resilience. Karaca et al. (2018) examine the reciprocal relationship between corporate governance and enterprise risk management (ERM) through a case study of the Borsa Istanbul Stock Exchange. Their findings reveal that strong governance mechanisms—such as board independence, audit committee oversight, and transparency policies—enhance ERM implementation by institutionalizing accountability and strategic alignment. In turn, robust ERM practices reinforce governance by improving risk visibility and decision-making across the enterprise. This mutual reinforcement reflects systems

thinking, as both governance and ERM are treated as interdependent subsystems whose feedback loops collectively influence organizational resilience. The case also highlights how systemic integration of governance and ERM enables proactive risk sensing and adaptive control structures, essential for complex financial infrastructures like stock exchanges (Karaca et al., 2018).

Karanja (2017) investigates whether the appointment of Chief Risk Officers (CROs) aligns with the structural and strategic intentions of the COSO and ISO ERM frameworks. The study finds that firms hiring CROs often demonstrate stronger alignment with key ERM principles, such as centralized risk oversight, strategic risk integration, and improved communication across business units (Karanja, 2017). CROs act as system integrators, ensuring that risk information flows across organizational silos and informs board-level decisions—an embodiment of systems thinking within governance structures. However, Karanja (2017) also notes that the CRO role's effectiveness depends on reporting lines, executive support, and organizational culture, highlighting that structural adoption alone does not guarantee systemic integration. Ultimately, the research affirms that embedding a CRO function can catalyze the feedback loops and cross-functional awareness necessary for ERM to function as a dynamic, enterprise-wide system (Karanja, 2017). Saleem, Zraqat, and Okour (2019) empirically investigate the influence of internal audit quality (IAQ) on the effectiveness of enterprise risk management (ERM) within the COSO framework, using data from firms in Jordan. The study finds a significant positive relationship between IAQ dimensions—such as auditor independence, competency, and objectivity—and the maturity of ERM implementation. High-quality internal audit

functions enhance feedback mechanisms within the organization by identifying emerging risks, ensuring control effectiveness, and promoting transparency. This reinforces systems thinking, as the audit function acts as a dynamic monitoring and learning subsystem within the broader ERM architecture. The findings suggest that internal audits not only support compliance but also help maintain the adaptive capacity of ERM through continuous evaluation and systemic oversight.

In conclusion, the synthesis of this extensive body of literature leads to several key takeaways. First, the structural transformation of financial markets, particularly the evolution from mutual to demutualized exchange structures, has introduced new complexities and governance challenges that demand innovative regulatory oversight (Dombalagian, 2020; Krueger, 2006; Aggarwal et al., 2007). Second, there is a clear shift toward cyber-resilience, emphasizing the need to move beyond purely preventive cybersecurity postures to resilience-based approaches capable of mitigating the long-term impacts of increasingly sophisticated cyber threats (Dupont, 2019; Gottipati, 2020; Johnson, 2015). Third, the development of integrated and strategic enterprise risk management (ERM) frameworks proves essential, as aligning ERM with organizational strategy enhances operational efficiency and positively influences firm value and market performance (Hoyt and Liebenberg, 2011; Lundqvist, 2014; Sax and Andersen, 2019). Fourth, the importance of systems thinking in risk management cannot be overstated, as it enables organizations to better capture interdependencies and dynamic interactions within their operational environments, leading to more adaptive and effective risk mitigation strategies (White, 1995; Salim, 2014; O'Donnell, 2005; Stave and Hopper, 2007). Fifth,

enhanced quantification and disclosure practices, particularly the measurement of residual cyber risks and the standardization of cyber risk disclosures, are critical to fostering transparent and effective risk management frameworks (Kountur, 2018; Gordon et al., 2011; Trautman and Newman, 2022). Finally, organizational culture and governance emerge as pivotal, with a risk-aware culture, strong corporate governance, and committed leadership being indispensable to embedding risk management as a core strategic function within institutions (Agarwal and Kallapur, 2018; Arena et al., 2010; Beasley et al., 2023; Stoll, 2015). Collectively, these insights highlight the evolving landscape of financial market infrastructures and underscore the necessity of a holistic, proactive approach to risk management.

2.9 Research Gaps

Based on the literature review, following areas can be further elaborated based on my research questions.

- Research Question 1: How can systems thinking be applied to cybersecurity risk management within the Enterprise Risk Management (ERM) framework of stock exchanges and clearing houses?
    - Fragmentation between ERM and Cybersecurity:

      Most literature (e.g., Romanosky and Petrun Sayers, 2021; Kurniawanti, 2010) highlights that cybersecurity is still treated as an IT silo rather than integrated into broader ERM, especially in financial market infrastructures.
    - Lack of Systems Thinking Application in Practice:

      While theoretical endorsements exist (e.g., Salim, 2014; O'Donnell, 2005),

there's limited empirical research demonstrating *how* systems thinking tools—like causal loop diagrams or feedback loops—are used in financial-sector risk governance.

- Research Question 2: What governance models can financial institutions adopt to balance cybersecurity risk governance?
    1. Insufficient Attention to Board-Level Cyber Risk Governance - Although Aebi et al. (2012) and Agarwal and Kallapur (2018) discuss CRO structures, there is limited exploration of how board-level decisions reflect cybersecurity trade-offs in market infrastructure entities.

Chapter III:

3. METHODOLOGY

This investigation adopts a qualitative research strategy rooted in systems thinking to explore how stock exchanges, designated clearing organizations (DCOs), and futures commission merchants (FCMs) can integrate cybersecurity into enterprise risk management (ERM) frameworks to preserve market stability. The methodology unfolds scoping, data collection, construct operationalization, data analysis, and validation.

In the scoping phase, the study identifies a purposive sample of institutions involved in financial market infrastructure or critical services. This includes national and stock exchanges, designated contract markets (DCMs), DCOs, FCMs, and relevant private-sector entities or regulatory bodies. Selection is based on the organizations' systemic relevance to the trading and clearing of financial instruments such as equities, options, and commodity futures.

Data collection is primarily conducted through semi-structured interviews with subject matter experts across cybersecurity, risk management, governance, and compliance functions. Each interview lasts approximately 60-90 minutes and is guided by a structured protocol. The interview questions are organized around four key constructs: systems thinking, ERM integration, cyber resilience, and regulatory compliance. Participants are encouraged to reflect on real-world practices, experiences and offer insights on specific topics, including the feedback loops between cyber threat detection and capital/resource allocation, definitions of ransomware risk tolerance, the use of cyber risk metrics at the

board level, and how past cyber incidents—whether disclosed or not—have shaped organizational responses.

To ensure triangulation and enrich the empirical base, the study also incorporates an analysis of secondary data sources. These include (a) publicly available incident reports related to cyber breaches affecting financial entities, (b) SEC Form 10-K and 8-K filings that disclose cybersecurity risks and incidents, and (c) governance charters and board committee mandates from publicly traded companies, particularly those that explicitly outline cyber oversight responsibilities.

The constructs derived from systems thinking—such as interdependencies, feedback mechanisms, and dynamic adaptation—are mapped to organizational risk management practices and are further discussed and assessed.

Based on the data points gathered in the interview; themes are first generated from the information shared and then analyzed in relation to existing literature on ERM, cyber governance, and regulatory frameworks.

Verification is conducted via participant feedback and member checks, whereby a subset of interviewees are invited to review synthesized findings to ensure representational accuracy and theoretical resonance. This rigorous, multi-layered methodology provides a robust foundation for understanding how financial institutions can embed cybersecurity into strategic ERM systems through the lens of systems thinking.

3.1 Research Design

A qualitative multiple-case study design (Yin, 2018) provides the overarching framework for this research because it allows for rich, contextualized comparisons of complex socio-technical systems while preserving the unique risk posture of each organization. To deepen the analysis, system-dynamics modeling (Sterman, 2000) is employed to transform qualitative insights into causal-loop diagrams, illustrating how cyber threats propagate through exchange and clearing-house ecosystems, how controls attenuate those threats, and how regulatory changes reverberate across feedback loops. The study adopts a pragmatist epistemology, which emphasizes an action-oriented approach where knowledge is judged by its effectiveness in addressing real-world problems. It embraces a flexible methodology that supports mixed-methods research, recognizing qualitative and quantitative evidence as equally valid if they contribute to problem-solving. Additionally, it adopts a pluralistic stance, accepting multiple ways of knowing—whether objective, subjective, or interpretive—depending on the context. Finally, the study is problem-centered, allowing the research question to drive the design rather than rigid adherence to a single methodological tradition, ensuring that the chosen methods are suited to addressing the practical challenges under investigation.

This study adopts qualitative analysis based on the review of published incidents, review of 10K and 8K SEC filings, governance charters, interviews and response analysis to provide a holistic view of cybersecurity risk management effectiveness.

Table 1

Data Collection Methods

Source	Rationale	Alignment to Research Questions (RQs)
Semi-structured interviews with CISOs, CIO, CTO, CROs, Compliance professionals, Technology-risk professionals	Capture lived experience of applying systems thinking, operationalizing regulatory controls, and designing governance mechanisms	RQ1, RQ2
Archival documents: SEC Form 10-K cyber-risk disclosures; SEC Reg SCI Rules; CFTC System Safeguards filings; incident post-mortems; board-committee charters SEC/CFTC Regulatory guidance and rules related to cyber security	Provide narrative about control environments and governance structures	RQ1, RQ2

Source	Rationale	Alignment to Research Questions (RQs)
Published Incidents and Threat Intelligence information: Various Cyber Security threat advisories, Verizon DBIR exchange sector cuts, and MITRE ATT&CK mappings	Summarization of threat landscape and inform system-dynamics parameterization	RQ2

3.2 Data Analysis

a) Compare findings across multiple responses to identify common cybersecurity risk management practices and challenges.

b) Analyze the information to propose a systems-based cybersecurity risk governance model, extend systems thinking applications in ERM and cybersecurity risk governance in terms of actionable step by step approach and offer recommendations for cybersecurity policies for market stability.

Chapter IV:

4 RESULTS

The research participants comprised a diverse group of highly experienced professionals, including C-level executives who report directly to corporate boards, Senior Compliance/Risk Directors, Cybersecurity Directors, and Security Operations personnel. These individuals bring extensive expertise across a range of financial market infrastructures, including multinational banks, equities exchanges, options exchanges, and futures and commodities exchanges, with broad experiences and perspectives on risk management and cybersecurity practices. On average, the C-level executives and directors have more than 25 years of experience in the domain and are active contributors to various industry risk management forums, recognized as established and credible professionals. The interviews were conducted in a semi-structured format to allow flexibility in exploring key themes while maintaining consistency across discussions. Given the sensitive nature of the topic and at the explicit request of the participants, the interviews were not recorded. Interviews were conducted using online meeting software, conference phone calls, or in-person sessions. Notes were taken as needed by hand during each session and subsequently summarized and generalized to protect participant confidentiality. Participants agreed to share their insights on the strict condition that they would not be quoted directly and that their organizations would not be explicitly named in any published findings. An interesting pattern emerged during the interviews—though not driven by gender bias but more by professional orientation and role context. Female professionals, particularly those in compliance and audit roles, tended to emphasize procedural rigor, regulatory alignment,

and audit preparedness. In contrast, male professionals, especially those with operational or strategic mandates, often framed discussions around trade-offs, critical success factors, and broader business impact. These contrasting yet complementary perspectives enriched the findings and offered a more holistic understanding of how organizations approach cybersecurity and risk governance. The interviewers themselves were primarily based in the United States and brought professional backgrounds in financial services and risk management, ensuring a nuanced understanding of the subject matter. This approach maintained the integrity and depth of the data while respecting the privacy concerns of the participants and ensuring that the insights collected were both candid and credible.

4.1 Research Question One

1. **RQ1) How Systems Thinking Can Be Applied to Cybersecurity Risk Management within the ERM Framework of Financial Institutions?**

Based on the various semi structured interviews, anecdotal information and the information collected, it is clear that adopting the following approach can help with better integration of cybersecurity risk management within the broader context of enterprise risk management:

- Translating Strategic Goals into Critical Success Factors (CSFs) - Systems thinking begins by connecting strategic business goals with measurable performance outcomes. Financial institutions can break down abstract objectives—such as "protect market integrity" or "ensure uninterrupted trade execution"—into concrete, testable CSFs (Critical Success Factors). These CSFs serve as focal points within the enterprise system, guiding all cyber-risk governance. They embody the principle

of emergence in systems thinking—where high-level outcomes arise from the interaction of multiple subsystems.

- Mapping Interdependencies Across People, Processes, and Technology - Systems thinking emphasizes interconnectedness. Institutions can use visual dependency maps to trace how workflows, applications, human roles, and infrastructure collectively support each CSF. These maps can expose hidden systemic risks—such as single points of failure or tightly coupled third-party services—that would otherwise be overlooked in siloed assessments. This holistic view aligns with systems thinking's focus on feedback loops and dynamic interactions.
- Establishing a Living CSF Register as a Systemic Anchor - The CSF register becomes a governance artifact that aligns cybersecurity practices with enterprise value creation. This register is not static; it evolves with system changes and integrates into DevSysops-SecOps, observability platforms, and risk workflows. It reflects systems thinking's emphasis on adaptability and continuous learning within complex systems.
- Embedding CSFs into Enterprise Risk Appetite Statements - By trying to translate CSFs into specific risk appetite statements (e.g., maximum downtime thresholds, latency ceilings), organizations transform abstract tolerances into operational limits. These thresholds help balance innovation and stability—capturing the tension between competing subsystems, a key insight from systems thinking. For example, faster product releases may increase fragility unless reconciled with platform reliability demands.

- Integrating CSFs with the Enterprise Risk Register (ERR) - Each inherent cyber risk is linked to its corresponding CSF and logged into the ERR. This ensures cybersecurity risks are evaluated alongside credit, market, and operational risks in a unified decision-making framework. Linking ERR status updates to CSFs reinforces systemic awareness—every risk is contextualized by its impact on the overall business system.
- Prioritizing Threat Intelligence Based on System Value - Systems thinking enables risk prioritization by evaluating threats through their impact on the system. Cyber threat intelligence is filtered through CSF alignment—only incidents that threaten critical pathways trigger immediate escalation. This value-driven triage mechanism reflects the systems principle of non-linearity—small attacks in the wrong place can cause outsized harm, which must be preemptively identified.
- Aligning Incident Response and Testing to CSFs - Red and blue team exercises simulate attacks on specific CSFs, enabling stress-testing of both resilience and recovery capabilities. System-wide scenarios—such as multi-region cloud failures or privilege escalations—are modeled to observe how quickly the institution can return within CSF thresholds. This aligns with the systems thinking principle of resilience over robustness, focusing on recovery dynamics, not just failure prevention.
- Creating Feedback Loops Between Technology, People, and Governance - Systems thinking relies on feedback. In mature institutions, telemetry from technology infrastructure, human performance (e.g., training effectiveness), and control

adherence (e.g., patch SLA violations) feeds back into ERR status updates and CSF performance dashboards. This continuous feedback allows the system to self-correct and mature—hallmarks of a learning organization.

- Informing Culture and Incentives Through Systemic Responsibility - In systems thinking, every part of the system shares responsibility for outcomes. Institutions embed CSFs into KPIs for developers, operations staff, risk officers, and executives. Bonuses and performance reviews reflect the shared goal of keeping the system within CSF-defined tolerances. This system-wide accountability reinforces collective resilience, not just localized compliance.
- Supporting Regulatory and Investor Disclosures with System-Based Metrics - Regulations like the SEC's 2023 Cybersecurity Governance Rule require firms to demonstrate how cyber risks affect critical services. Systems thinking provides traceability from board-level objectives to operational outcomes, backed by CSF-aligned metrics. This strengthens trust and transparency with regulators, investors, and customers.
- Enabling Sector-Wide Systemic Risk Management - Financial institutions operating in interconnected markets can use CSFs and system-mapping to contribute to sector-wide resilience. Sharing sanitized dependency maps and failure scenarios (via FSISAC or regulatory collaboration) reflects systems thinking's application at the macro level—treating financial markets as ecosystems where interdependencies can amplify or contain systemic shocks.

Applying systems thinking to cybersecurity risk management within ERM allows financial institutions to transcend fragmented, compliance-driven approaches and build a dynamic, interconnected, and resilient enterprise. By anchoring risk practices to CSFs, modeling system dependencies, and embedding cyber risks into unified governance frameworks, institutions not only protect themselves but also strengthen trust in the broader financial ecosystem. Each CSF becomes a focal lens for understanding how technology, people, and processes collaborate—or conflict—to deliver secure, uninterrupted value in an increasingly complex threat environment. Systems thinking transforms cybersecurity risk management into a dynamic, interconnected discipline, enabling financial institutions to manage risks proactively. Based on this research, the following steps effectively integrate cybersecurity into

4.1.2 ERM using systems thinking

Mapping Business Objectives to System and operational environment dependencies:

1. Identify how strategic business goals translate into processes, workflows, and technology systems.

This can be accomplished by:

- Clear formulation of the key business strategic goals and critical success factors.
- Identification and mapping of key business process to the organizational deliverables and supporting systems that directly map to the business process.

- Clear documentation of critical resources in terms of People, Process and Technology that are on critical path to support an end-to-end business process.
- Identification and documentation of the key critical success factors for those systems and supporting operating environments.

2. Identification and documentation of inherent risks.
    - Evaluate the technical architecture, data classification and supporting operation environment and document inherent risks that are relevant for a given ecosystem
    - Each inherent risks that will negatively affect the critical success factor that is deemed relevant should be included in the formal risk register
    - Each inherent risk must be evaluated for inherent likelihood (how probable a given event is considering internal and external environments and general threat landscape) and impact for that event
    - Explain these inter-dependencies clearly to enable stakeholders to comprehend systemic impacts of cybersecurity incidents across the enterprise.

Below is a visual representation illustrating how systems thinking can be applied practically to cybersecurity risk management within ERM frameworks.

Figure 1

Organizational Systems thinking linkage

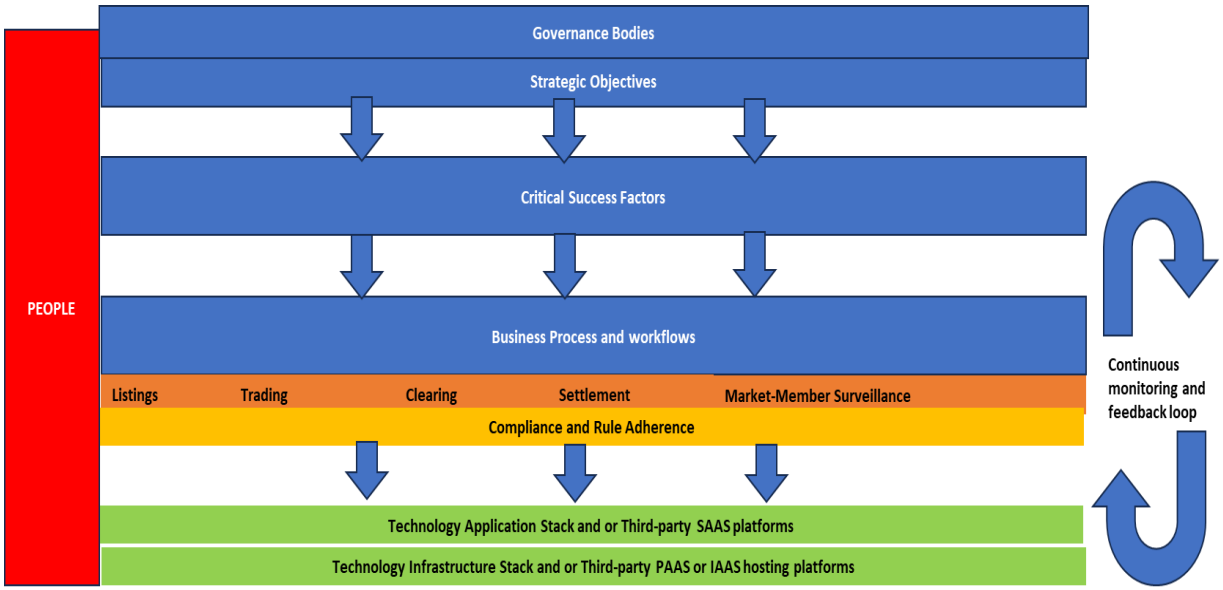

Table 2

Organizational Systems thinking linkage description

1. Start at the Top – Strategic Objectives	At the highest level, financial institutions articulate strategic objectives such as maintaining market trust, ensuring uninterrupted trading, or complying with SEC cybersecurity rules. These are broad goals that guide the institution's direction. **Link to systems thinking:** Strategic objectives are the emergent properties of a well-functioning system. They're only achievable when all system components—people, processes, technology—are aligned and resilient. Strategic objectives are best understood as emergent

	properties because they arise not from the isolated actions of individuals or departments but from the coordinated, integrated operation of the entire organizational system. In systems thinking, emergent properties are outcomes that cannot be attributed to any single component but instead result from the complex interactions between components. In a business context, achieving strategic objectives—such as market leadership, operational efficiency, or innovation—depends on the synergy between people, processes, and technology. If any one of these elements is misaligned or underperforming, it introduces friction or vulnerabilities that can derail organizational goals. For example, even with cutting-edge technology, if the workforce lacks the necessary skills or if business processes are inefficient, the strategic goals cannot be realized. Similarly, resilient systems are necessary because they can adapt to disruptions, mitigate risks, and sustain progress toward strategic aims even under pressure.
2. Move Down to Critical Success Factors (CSFs)	To make strategy actionable, we define Critical Success Factors (CSF) — example measurable outcomes like sub-100 microsecond trade matching or five-minute maximum recovery time after disruption. **Link to systems thinking:** CSFs help us trace cause and effect. They create feedback loops

	between strategic goals and the actual performance of sub-systems, showing where gaps can lead to systemic failures. The connection to systems thinking is fundamental. In a complex system, outcomes are not the result of isolated actions but of interdependent processes and feedback mechanisms. CSFs function as key indicators within this system, helping organizations trace cause-and-effect relationships between strategic goals and operational performance. When CSFs are properly defined and monitored, they create feedback loops: performance data feeds back to management, highlighting how well each sub-system is functioning in support of the broader strategy. These loops allow leaders to identify gaps early—where underperformance in one area, like slower trade matching, can cascade into larger systemic failures, such as market inefficiencies or regulatory breaches. By embedding CSFs into the system's feedback structure, organizations can detect misalignments between strategy and operations and make timely adjustments. This approach ensures that strategy remains a living, adaptive framework rather than a static plan. Thus, CSFs are not just performance metrics; they are the mechanisms that maintain the dynamic balance of the system, driving continuous alignment

	and resilience, both of which are central principles in systems thinking.
3. Connect to Business Processes and Workflows	Business functions—like trading, settlement, surveillance—are the operational engines that deliver these CSFs. If one breaks, the CSF fails. **Link to systems thinking:** These processes are interconnected nodes in the system. A cyber risk affecting one (e.g., Ransomware attack on systems) can propagate downstream and compromise multiple CSFs. Business functions such as trading, settlement, and market surveillance act as the operational engines that deliver on an organization's Critical Success Factors (CSFs). Each function contributes directly to achieving key measurable outcomes; for example, fast and accurate trade matching or timely settlement clearance. However, if any one of these critical functions fails—whether through technical malfunction, human error, or cyberattack—the CSF it supports is immediately at risk of failure. From a systems thinking perspective, these business functions are not isolated units but interconnected nodes within a larger, complex organizational system. Disruptions in one node can have cascading effects across the system. For instance, a ransomware attack targeting settlement systems may not only delay the

	settlement process but also create a ripple effect that disrupts trade reconciliation, reporting, and regulatory compliance, thereby compromising multiple CSFs simultaneously. Systems thinking emphasizes understanding these interdependencies and feedback loops, illustrating how vulnerabilities in one part of the system can propagate downstream and amplify risks elsewhere. This interconnected view highlights the importance of designing resilient, adaptive systems where risk management is not confined to individual functions but is embedded across the entire network of business operations. Ensuring that all nodes are robust and that contingencies are in place allows organizations to better protect their CSFs, maintain operational integrity, and fulfill their strategic objectives even under adverse conditions.
4. Highlight Compliance and Governance	Compliance ensures that every process operates within regulatory boundaries. Failure to comply—say, a missed trade report due to cyber interference—can damage credibility and attract penalties. **Link to systems thinking:** Compliance and Governance acts as a control mechanism—a balancing loop that regulates behavior and keeps the system within safe operational limits. Compliance plays a critical role in ensuring that every business process operates within established regulatory boundaries, safeguarding the integrity and credibility

	of financial institutions. When compliance fails—such as a missed trade report caused by cyber interference—it can lead to significant consequences, including reputational damage, regulatory penalties, and loss of stakeholder trust. From a systems thinking perspective, compliance functions as a control mechanism, akin to a balancing loop that regulates organizational behavior and keeps the entire system operating within safe and acceptable limits. Just as feedback loops in complex systems help maintain stability by counteracting deviations, governance and compliance structures monitor operational activities and correct course when risks or non-conformities emerge. These balancing loops are essential to preventing systemic drift, where unchecked small failures can accumulate and lead to large-scale breakdowns. By continuously feeding compliance data back into decision-making processes, organizations ensure that operational activities remain aligned not only with internal policies but also with external regulatory expectations. In this way, compliance is not a static checklist but a dynamic regulatory force that contributes to the system's resilience and long-term sustainability.
5. Dive into Technology and	Below the business workflows lie the tech platforms—SaaS, PaaS, IaaS—and the infrastructure that makes everything run.

Infrastructure Layers	These are critical for uptime, data integrity, and real-time performance. **Link to systems thinking:** These layers form the system's foundation. Systems thinking urges us to model their interactions and dependencies—because a flaw here (e.g., cloud misconfiguration or single point of failure) can ripple upward and impact strategic outcomes. Beneath business workflows lie the critical technological platforms— Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) along with the underlying infrastructure that powers every operational and strategic function. These technology layers are essential for ensuring uptime, maintaining data integrity, and supporting real-time performance requirements. Without their stable operation, business functions cannot reliably deliver on Critical Success Factors (CSFs). From a systems thinking perspective, these technology layers form the foundation of the organizational system. Systems thinking urges us to model the interactions and dependencies among these platforms and the workflows they support because disruptions at this foundational level—such as a cloud misconfiguration, a hardware failure, or a single point of failure—can ripple upward, impacting not just isolated operations

	but the achievement of broader strategic outcomes. A systems model reveals that the resilience and proper design of these foundational components are not merely IT concerns but are central to sustaining the health and performance of the entire enterprise. Understanding and managing these interdependencies proactively ensures that risks are addressed at their roots, rather than reacting only when systemic failures become visible at the surface level.
6. Emphasize the Role of People	People are embedded in every layer—setting goals, interpreting data, responding to incidents, and configuring systems. Human error, knowledge gaps, or skill shortages can destabilize the entire system. **Link to systems thinking:** Systems thinking treats organizations as socio-technical systems—humans and machines together create outcomes. This perspective helps us model cyber risk not just as a technical problem, but as a human–machine dynamic. People are embedded across every layer of an organization, playing critical roles in setting goals, interpreting data, responding to incidents, and configuring systems. Their decisions and actions directly influence the reliability and security of both business operations and the underlying technology. However, human error,

	knowledge gaps, and skill shortages can destabilize even the most well-designed systems, introducing vulnerabilities that technology alone cannot eliminate. Systems thinking views organizations as socio-technical systems, where humans and machines interact in complex, interdependent ways to create outcomes. This perspective emphasizes that cyber risk is not purely a technical problem but a human–machine dynamic. By modeling these interactions, systems thinking allows organizations to identify where breakdowns can occur, whether due to poor interface design, inadequate training, or decision fatigue. It encourages a holistic approach to risk management, one that incorporates human behavior, organizational culture, and technological dependencies into the assessment and mitigation of cyber threats. Recognizing people as integral nodes in the system strengthens resilience by addressing both the technical and social dimensions of risk.
7. Illustrate Feedback Loops and Adaptation	The curved arrows show how the system responds and learns. Incidents feed back into governance, new policies adjust risk appetite, and threat intelligence updates configurations. **Link to systems thinking:** Feedback is at the heart of systems thinking. It enables dynamic adjustment to threats—making cybersecurity proactive, not just

	reactive. The curved arrows in a systems model illustrate how the organization responds and learns over time. Cybersecurity incidents feed back into governance structures, prompting adjustments to policies and influencing the organization's risk appetite. Simultaneously, new threat intelligence leads to updates in system configurations and security controls. This continuous flow of information and adaptation highlights the dynamic nature of modern cybersecurity operations. From a systems thinking perspective, feedback is fundamental—it is what allows the system to adjust dynamically in response to internal failures and external threats. Without feedback loops, organizations remain reactive, merely responding to incidents after damage has occurred. With feedback integrated, cybersecurity becomes proactive, enabling the system to evolve and strengthen before vulnerabilities are exploited. In this way, feedback transforms cybersecurity from a static defense mechanism into a living, adaptive system that learns, adjusts, and becomes more resilient over time.

This model shows cybersecurity not as a static checklist but as a living system—interconnected, adaptive, and driven by strategic intent. Systems thinking gives us the

language, tools, and mindset to manage cybersecurity in a way that's integrated into enterprise risk—not separate from it.

Applying the systems thinking framework illustrated in the diagram, stock exchanges can adopt a defense-in-depth posture that aligns cybersecurity controls with the consistent accomplishment of Critical Success Factors (CSFs). This approach ensures strategic objectives such as "uninterrupted trading," "market integrity," and "regulatory compliance" are not only protected but continuously achieved even under cyber stress.

- Strategic Alignment of Defense-in-Depth - Strategic alignment is essential for an effective defense-in-depth approach, starting with explicitly tying cybersecurity controls to critical business outcomes. In the context of a stock exchange or clearing organization, Critical Success Factors (CSFs) such as sub-second trade execution, zero data loss in clearing and settlement, 24x7 system availability, and maintaining a flawless regulatory compliance record define operational success. These CSFs are not just technical benchmarks but fundamental drivers of organizational credibility and market stability. Therefore, the security architecture must be deliberately designed to prioritize the integrity, availability, and confidentiality of the systems and processes that underpin these outcomes. By ensuring that cyber defenses are mapped to business priorities, organizations can create a multi-layered security posture that not only protects against threats but also safeguards the mission-critical operations that directly influence their strategic objectives. This alignment elevates defense-in-depth from a purely technical exercise to a business-driven imperative, ensuring that cybersecurity investments deliver tangible support for the organization's broader goals.

- Prevention-Focused Controls by Layer - A comprehensive defense-in-depth strategy requires applying prevention-focused controls systematically across multiple layers of the organization. Starting with people, organizations must enforce role-based access control (RBAC) and the principle of least privilege, deliver targeted security training tailored to specific workflows such as trading desk phishing simulations, and implement continuous background screening for privileged users. At the process and workflow level, it is essential to embed security by design through secure development lifecycle (SDLC) practices for trading applications and apply zero-trust principles by requiring re-authentication for high-value operations. Advanced measures like pre-trade risk filters and machine learning-driven anomaly detection further strengthen workflow defenses. For compliance and governance, codifying Critical Success Factors (CSFs) into formal policies—such as maintaining a 100-microsecond latency threshold for the matching engine—ensures strategic alignment. Automated GRC platform integration for controls testing and real-time alerting ensures immediate responses to policy violations tied to CSFs. Within the technology stack, proactive measures include patching and hardening SaaS, PaaS, and IaaS environments, employing micro segmentation and application firewalls to isolate critical trading and clearing flows, and encrypting data in motion and at rest. Finally, the infrastructure layer must feature resilient configurations, such as active-active failover for DNS, NTP, and load balancers, the deployment of hardware security modules (HSMs) for safeguarding transaction chain cryptography, and preconfigured DDoS protections on peering links and trading gateways. By applying layered, prevention-

focused controls, financial organizations not only reduce the attack surface but also reinforce the operational resilience necessary to support high-stakes business functions.

- Resilience Controls: Prepare, Absorb, recover - Stock exchanges must operate under the assumption that breaches are inevitable and must design resilience controls capable of detecting, containing, and recovering from incidents without violating Critical Success Factors (CSFs). In the prepare phase, exchanges may run red team exercises simulating high-impact CSF failures, such as halted trading sessions, maintain CSF-specific recovery playbooks, conduct Recovery Time Objective (RTO) drills, and integrate real-time observability platforms with incident response dashboards to ensure rapid situational awareness. During the absorb phase, resilience requires hot/hot failover architectures for order matching engines and core clearing systems to maintain uninterrupted operations, while isolating environments—such as trading platforms and back-office reporting systems—to prevent cross-contamination. In parallel, the deployment of real-time behavioral analytics can enable early detection and containment of abnormal transaction flows, limiting the spread of potential attacks. Finally, the recovery phase emphasizes the automation of recovery processes tied to CSF-linked Recovery Point Objectives (RPOs) and RTO thresholds. This includes deploying redundant and diverse backup pipelines for critical market and clearing data and continuously reassessing recovery times to ensure alignment with the organization's CSF-driven risk appetite statements. Together, these layered resilience measures create a robust framework that not only mitigates the impact of cyber incidents but ensures that the exchange’s essential business functions can continue without breaching their strategic commitments.

- Measuring Control Effectiveness via CSFs - To ensure cybersecurity efforts are aligned with business outcomes, CSF telemetry—such as latency, error rates, and system uptime—should feed directly into control dashboards, providing real-time visibility into the health of Critical Success Factors. Every control implemented must have a clear and explicit purpose: to prevent the breach or degradation of a specific CSF. For instance, firewall uptime directly supports the trade availability CSF, ensuring continuous access to trading platforms. Hardware Security Module (HSM) policy adherence reinforces the data integrity CSF, safeguarding transaction authenticity, while regular backup restore testing feeds into the settlement continuity CSF, ensuring that critical clearing functions can recover swiftly after disruption. This direct mapping of controls to CSFs avoids the trap of deploying "controls for control's sake" and ensures that cybersecurity investments are tightly focused on protecting the systems and processes that create the most strategic value for the organization. By maintaining this alignment, organizations maximize both security effectiveness and operational efficiency.
- Feedback Loops and System Learning - Incident reviews must go beyond diagnosing immediate failures to examine which Critical Success Factors (CSFs) were threatened and why. A deeper analysis requires understanding how a breakdown in one area can propagate through the system, using dependency maps to trace cascading failures—for example, how a bad market data in trading systems could ultimately result in a regulatory breach due to erroneous trades. This interconnected view ensures that risk management efforts are not isolated but systemic. Following each review, organizations should update the CSF register and Enterprise Risk Register (ERR) based on lessons

learned about control effectiveness and evolving threats. By continually refining these critical documents, institutions ensure that their defense posture adapts in response to real-world challenges, maintaining resilience and strategic alignment over time.

4.1.3 Conclusion

Defense-in-depth, when viewed through a systems thinking lens, becomes more than just layered security—it becomes mission alignment. Each control layer defends the integrity of workflows, people, and technologies that uphold the stock exchange's strategic objectives. Prevention keeps systems safe, and resilience ensures they recover—both working in harmony to ensure CSFs are consistently met even in the face of evolving cyber threats.

4.2 Research Question Two

RQ2) What governance models can financial institutions adopt to balance cybersecurity risk governance?

The data reveals several consistent themes that inform the design and implementation of effective governance structures for cybersecurity within ERM. The responses overwhelmingly emphasize the integration of cyber risk into broader enterprise governance structures through cross-functional collaboration, board-level visibility, and formalized disclosure protocols. The insights have been organized under key categories that reflect practical governance enablers.

- Recognition of Cybersecurity as a Business Risk - A unanimous response across interviewees was the belief that cybersecurity is no longer a siloed IT problem but a fundamental business risk with the potential to impact an organization's core objectives. Respondents stressed that the traditional model—where cyber risk is managed exclusively by the CISO or security team—is no longer sufficient. Participants consistently tied cyber threats to disruption in business operations, legal liability, reputational damage, and loss of market share.This recognition mandates that cyber risk must be governed as a first-class risk category in the ERM framework. Several organizations have already implemented ERM dashboards where cyber metrics sit alongside credit, market, and operational risk indicators, often mapped to Critical Success Factors (CSFs) such as “24/7 system availability,” “no unauthorized data exposure,” or “trade execution integrity.”
- Establishment of Cross-Functional Cyber Risk Committees - Nearly all respondents emphasized the importance of forming cross-functional cyber risk committees that meet on a monthly or quarterly basis as an integral part of the broader Enterprise Risk Management (ERM) steering group. These committees should be composed of representatives from Risk Management, Information Security, IT and Infrastructure, Legal and Compliance, Business Unit Leadership, and Investor Relations or Corporate Communications. Importantly, respondents noted that the committee’s role should extend beyond a purely advisory function. It must be empowered to actively review the organization’s cyber risk posture against its established enterprise risk appetite, approve remediation roadmaps, evaluate third-party risks, and coordinate materiality assessments for regulatory disclosures. In some organizations, this structure has been further strengthened by formally establishing the

committee under the authority of the board's audit or risk sub-committee, ensuring direct oversight and greater continuity in governance practices.

- Mapping Cybersecurity to Critical Success Factors (CSFs) - A key governance practice highlighted by interviewees is the alignment of cybersecurity risks to Critical Success Factors (CSFs). This alignment enables governance bodies to pose a crucial question: which cybersecurity failures could directly compromise the organization's ability to deliver core services? Specific examples cited include "sub-millisecond trade matching latency" as a CSF vulnerable to disruptions like DDoS attacks or infrastructure failures; "no material customer data breach" as a CSF at risk from application-level vulnerabilities; and "regulatory filing accuracy," which hinges on robust data integrity and access controls. By linking cyber threats to essential business outcomes, organizations can make risk discussions more tangible and relevant, particularly for senior leaders who may not have a technical background.
- Cyber Metrics and Dashboard Reporting - Survey respondents emphasized the critical role of integrating cybersecurity metrics into Enterprise Risk Management (ERM) dashboards. Key metrics identified include system availability and recovery times (RTO/RPO), patch compliance rates, endpoint protection coverage, the number and severity of incidents over time, and control testing results mapped to frameworks such as NIST CSF or ISO 27001. Boards and executives noted that dashboards using red-yellow-green thresholds, aligned with Critical Success Factors (CSFs), help focus executive attention on the organization's true risk posture. Several organizations have advanced this practice by implementing automated data feeds from Security Information and Event

Management (SIEM) or Governance, Risk, and Compliance (GRC) tools into their ERM dashboards, making cybersecurity risk reviews a standard component of quarterly board reporting.

- Governance through Disclosure: 10-K and 10-Q Integration - A powerful governance lever identified by both internal and external stakeholders is the formal disclosure of cybersecurity risks in regulatory filings. The majority of interviewed respondents supported incorporating cybersecurity risk posture into 10-K (annual) and 10-Q (quarterly) reports. They referenced SEC guidance that encourages public companies to disclose how cybersecurity is governed, the roles of the board and senior management in oversight, material incidents and response strategies, and the integration of cyber risk into strategic planning. Interviewees observed that formal disclosure imposes greater rigor on internal governance because public statements must be verifiable. Discussions made it clear that once cybersecurity posture becomes part of the 10-K, organizations are compelled to design and implement more formalized control processes and governance mechanisms, leading to stronger alignment between cybersecurity management and business impact.
- Scenario Planning and Materiality Evaluation for 8-K Disclosures - Several organizations have established governance procedures for evaluating incident materiality using cross-functional response teams. These groups include Legal, InfoSec, Risk, Communications, and Investor Relations. They simulate likely attack scenarios (e.g., ransomware, insider threats) and pre-plan the response thresholds for 8-K filings under Item 1.05 (Material Cybersecurity Incident). This formalized escalation model ensures that if a cyber incident occurs, governance is not improvised. Surveyed respondents shared that

clearly defined playbooks reduce decision paralysis and help fulfill the “within four business days” requirement.

- Third-Party Cyber Risk Governance Models - The governance of vendor and partner risk emerged as a critical issue among respondents. Recommendations included maintaining a third-party risk register, requiring vendors to provide SOC 2 Type II or ISO certifications, embedding cybersecurity obligations into contracts through service level agreements (SLAs) and breach notification clauses, and reviewing third-party incident response procedures during onboarding. At the governance level, several organizations have elevated third-party cyber risk as a recurring agenda item in both cybersecurity committee meetings and board risk reports, reflecting its growing significance in overall risk management frameworks.
- Board-Level Oversight and Committee Integration - Participants widely agreed that strong board oversight is essential for effective cybersecurity governance. Several governance models were identified, including the establishment of a standalone cybersecurity committee at the board level (less common) and the more typical integration of cybersecurity risk discussions into the board’s existing risk or audit committee agendas. Many organizations also conduct quarterly briefings from the Chief Information Security Officer (CISO) and Chief Risk Officer (CRO) to update the board on cybersecurity posture and emerging threats. Respondents stressed the importance of boards viewing cybersecurity as a dynamic, systemic risk, especially as regulatory bodies like the SEC and CFTC increase their focus on board accountability. Ongoing board member training and

awareness programs, particularly those highlighting cyber scenarios with direct business impact, were seen as essential to ensuring directors fully grasp what is at stake.

- Culture of Shared Accountability - Finally, interview data emphasized the role of organizational culture. Effective governance requires not only structure but shared responsibility across first, second, and third lines of defense. Respondents cited examples like:
    - Including cyber risk in performance KPIs for product and tech teams
    - Aligning incentives across compliance, security, and operations
    - Conducting tabletop exercises that involve all lines of business

Organizations that fostered this shared accountability culture reported higher resilience, faster response times, and better regulatory outcomes.

4.2.1 Conclusion

The results clearly suggest that effective cybersecurity governance within ERM requires an integrated, systems thinking approach. Governance models must go beyond compliance checklists and focus on aligning cyber risk with enterprise value through cross-functional committees, formal board oversight, metrics integration, and regulatory disclosure. The most mature organizations implement governance not as a yearly policy review, but as a dynamic, feedback-driven practice. They leverage CSFs, dashboards, scenario planning, and formal disclosures to align cyber with strategy. As threats evolve, so must governance. The evidence suggests that cybersecurity is not just a subset of operational risk—it is a board-owned strategic concern requiring embedded, enterprise-wide governance.

4.3 Summary of Findings

RQ1) How Systems Thinking Can Be Applied to Cybersecurity Risk Management within the ERM Framework of Financial Institutions?

- Systems thinking enhances cybersecurity risk management in financial institutions by integrating cyber risks into the broader ERM framework, treating them as strategic business risks alongside credit, market, and operational risks. It encourages a holistic view by establishing cross-functional cyber risk committees that bring together Risk, IT, Legal, Business Units, and Communications, ensuring diverse perspectives and shared accountability. Cyber threats are mapped to Critical Success Factors (CSFs), such as system uptime and data confidentiality, aligning technical risks with business outcomes to make risk discussions relevant to leadership. Cybersecurity metrics are incorporated into ERM dashboards using visual traffic-light indicators to enable quick, informed decision-making. Formal disclosures in 10-K and 10-Q filings enforce governance rigor, driving alignment between cyber controls and business objectives. Additionally, scenario planning for regulatory disclosures (e.g., 8-K events) ensures institutions are prepared to respond to material incidents within required timeframes. Overall, systems thinking fosters interconnected governance structures that proactively manage cyber risks as an integral part of organizational resilience and strategic planning.

RQ2) What governance models can financial institutions adopt to balance cybersecurity risk governance?

- Effective governance models treat cybersecurity as a strategic business risk integrated into the ERM framework. Institutions establish cross-functional cyber risk committees to review posture and disclosure materiality, while cyber threats are mapped to Critical Success Factors (CSFs) to align risks with business priorities. Embedding cyber metrics into ERM dashboards and formalizing disclosure in 10-K/10-Q filings enhances transparency and accountability. Third-party risks are managed through continuous assessments and governance oversight. Board-level integration—either through risk/audit committees or dedicated cyber committees—ensures informed oversight, supported by regular briefings and training. Cyber risk input is embedded early in strategic decisions, and a culture of shared accountability across all lines of defense strengthens resilience and governance discipline.

Table 3

Summary of findings

RQ1) How Systems Thinking Can Be Applied to Cybersecurity Risk Management within the ERM Framework of	Systems thinking embeds cybersecurity within the Enterprise Risk Management framework, treating it as a strategic business risk alongside credit, market, and operational risks. By aligning cyber threats to Critical Success Factors and fostering cross-functional governance, it ensures risk discussions are relevant to leadership and tied to business

Financial Institutions?	outcomes. Integrated dashboards, formal disclosures, and scenario planning further strengthen resilience and readiness for regulatory reporting.
RQ2) What governance models can financial institutions adopt to balance cybersecurity risk governance?	Effective governance models integrate cybersecurity into the ERM framework, aligning threats with Critical Success Factors and business priorities. Cross-functional committees, embedded metrics in ERM dashboards, formal disclosures, and continuous third-party risk oversight enhance transparency and accountability. Board-level integration, early cyber risk input in strategic decisions, and a culture of shared accountability across all lines of defense strengthen resilience and governance discipline.

4.4 Conclusion

The findings reveal that effective cybersecurity governance demands a systems thinking approach, where cyber risk is not isolated but viewed as part of an interconnected enterprise ecosystem. By aligning cybersecurity with Critical Success Factors (CSFs), engaging cross-functional committees, and integrating cyber metrics into ERM dashboards and regulatory disclosures, institutions foster a feedback-driven, dynamic governance model. Systems thinking enables organizations to see how cyber threats impact strategic outcomes across technology, operations, legal, and reputational domains. This approach

also supports proactive decision-making through scenario planning, third-party oversight, and early cyber involvement in strategic initiatives. Ultimately, embedding cyber governance into ERM as a systemic, enterprise-wide concern improves organizational resilience, ensures regulatory alignment, and reinforces cybersecurity as a driver of sustained business value.

Chapter V:

5.0 DISCUSSION

5.1 Discussion of Results

The results of this study indicate a significant evolution in how financial institutions conceptualize and govern cybersecurity risks. Traditionally treated as a technical or IT concern, cybersecurity has now been recognized as a systemic business risk with profound implications for operational continuity, market reputation, legal compliance, and investor confidence. This transformation is driven not only by the increasing frequency and sophistication of cyber threats but also by regulatory expectations and stakeholder demands for transparency. In response, leading institutions are moving toward governance models that embed cybersecurity within the broader enterprise risk management (ERM) framework using a systems thinking approach. Systems thinking—defined by the holistic evaluation of interrelated components, feedback loops, and dynamic complexity—provides a valuable lens for integrating cyber risk into enterprise governance. Rather than viewing cyber threats in isolation, institutions are increasingly mapping these risks to strategic business objectives and critical success factors (CSFs), enabling more relevant and effective oversight at the executive and board levels.

One of the most prominent themes emerging from the data is the recognition of cybersecurity as a first-class business risk. Interviewees consistently emphasized that treating cyber risk as an isolated IT function creates blind spots in enterprise decision-making. When systems thinking is applied, cybersecurity is seen as a determinant of the organization's ability to deliver on its mission-critical outcomes—ranging from trade

execution integrity and data confidentiality to system uptime and regulatory accuracy. This shift in mindset allows risk to be contextualized in terms of business impact rather than technical failure. For example, mapping cyber threats such as ransomware or distributed denial-of-service (DDoS) attacks to business functions like customer onboarding or trading platform availability makes it easier for non-technical leaders to understand the urgency and scope of required controls. By doing so, institutions foster cross-functional dialogue and shared accountability, which are hallmarks of effective systems-based governance.

The establishment of cross-functional cyber risk committees further reinforces the systems thinking model. Rather than siloed governance within the IT or security department, these committees integrate representatives from risk management, legal, compliance, infrastructure, communications, and business units. This composition ensures that cyber risk decisions are informed by diverse perspectives, reflecting the interconnectedness of enterprise operations. These committees do not serve a purely advisory role; rather, they are empowered to evaluate cyber risk appetite, oversee remediation efforts, monitor third-party exposures, and guide regulatory disclosures. Moreover, some organizations have structured these cyber risk committees under the board's audit or risk sub-committees, institutionalizing cyber oversight at the highest level. This structure not only aligns with regulatory best practices but also creates a formal mechanism for cascading risk information across the enterprise—a key tenet of systems thinking.

Another critical finding is the importance of aligning cyber risks with Critical Success Factors (CSFs), which are used to define and track the performance of enterprise

objectives. CSFs such as “no unauthorized data exposure,” “99.99% system availability,” or “real-time regulatory reporting accuracy” provide tangible reference points for discussing cyber risks in terms of business impact. By linking cyber controls to these CSFs, organizations create a common language across IT, business, and executive leadership. This alignment also allows for the prioritization of cybersecurity investments based on the potential to disrupt key business outcomes. For instance, if a particular CSF is dependent on real-time data integrity, then investments in data access controls, encryption, and anomaly detection systems are not just justified—they become strategic imperatives. This systems-level mapping of cyber risk to business value strengthens accountability and drives more rational resource allocation.

Cybersecurity metrics and dashboard reporting also play a pivotal role in reinforcing a systems-oriented governance model. Institutions have increasingly embedded cyber metrics into enterprise risk dashboards, where they sit alongside financial, operational, and compliance indicators. These metrics—such as system uptime, patch management compliance, endpoint protection coverage, incident volume, and control maturity scores—are visualized using red-yellow-green thresholds to alert executives to deviations from acceptable risk tolerance levels. Importantly, several organizations have automated data feeds from their security information and event management (SIEM) and governance, risk, and compliance (GRC) platforms into these dashboards, making risk posture assessment an ongoing, real-time exercise. These feedback loops are central to systems thinking, allowing for dynamic adjustments in controls and resourcing as risks evolve.

Another area where systems thinking enhances governance is through regulatory disclosure. The integration of cybersecurity risk management details into 10-K and 10-Q filings imposes a level of discipline and accountability that internal reporting alone cannot achieve. Because these disclosures must be accurate and verifiable, they necessitate formal governance structures, evidence-based metrics, and cross-functional validation. The act of preparing these filings compels organizations to assess their cyber risk posture holistically and to establish governance mechanisms that can withstand external scrutiny. Furthermore, several institutions are adopting scenario-based planning and materiality evaluations to prepare for 8-K disclosures in the event of a material cybersecurity incident. By simulating high-impact scenarios like ransomware attacks or data breaches, cross-functional response teams are able to predefine escalation paths, communication protocols, and disclosure thresholds. This preparation minimizes decision paralysis during actual incidents and ensures that governance responses are timely and coordinated.

Vendor and third-party cybersecurity governance has also emerged as a critical component of systems-based ERM integration. Financial institutions increasingly depend on complex supply chains and digital ecosystems, making third-party risk a systemic issue rather than a peripheral concern. Respondents highlighted practices such as maintaining third-party risk registers, requiring SOC 2 or ISO 27001 certifications, embedding cybersecurity clauses in contracts, and conducting onboarding assessments of vendor response capabilities. At the governance level, third-party cyber risk is now a standing agenda item in cyber committees and board risk reports, further validating its role in

enterprise resilience. This broader perspective aligns with systems thinking, which stresses the importance of understanding external dependencies and feedback loops.

The role of the board is central to the success of any cybersecurity governance model. Institutions that are most advanced in this space have integrated cyber risk discussions into board risk or audit committees, ensuring consistent oversight from the top. Some have even created standalone cybersecurity committees, although this remains rare. Quarterly board-level updates by the CISO and Chief Risk Officer (CRO) are becoming standard practice, and many institutions now provide board training on cyber risk awareness. These practices reflect a recognition that cybersecurity is a dynamic, enterprise-wide issue that requires continuous engagement, not episodic attention. From a systems thinking standpoint, the board acts as a strategic node in the governance network, facilitating alignment between risk appetite, investment decisions, and enterprise outcomes.

Lastly, the development of a culture of shared accountability is essential for sustaining effective cybersecurity governance. Institutions that have embedded cyber risk awareness into performance metrics, incentive structures, and operational routines report stronger alignment across the three lines of defense. Regular tabletop exercises, phishing simulations, and post-incident reviews involving all business units reinforce this culture and create learning loops that improve future responses. Systems thinking underscores the value of such organizational learning processes, emphasizing adaptation and resilience over rigid compliance.

In conclusion, the findings affirm that a systems thinking approach offers a robust framework for embedding cybersecurity into ERM. This model promotes a dynamic,

feedback-driven governance environment that aligns cybersecurity with business strategy, regulatory expectations, and operational execution. By recognizing cyber risk as an enterprise concern and institutionalizing cross-functional governance, financial institutions enhance their ability to anticipate, withstand, and recover from evolving threats. As the cyber threat landscape continues to evolve, governance models must remain agile, systemic, and deeply integrated into the enterprise risk fabric.

5.2 Discussion of Research Question One

Critical Success Factors (CSFs, are deeply intertwined with systems thinking because they serve as the anchor points that connect the organization's strategic vision to its operational reality through a holistic, interdependent lens. Systems thinking emphasizes understanding the organization as a complex network of interconnected parts—people, processes, technologies, and external partners—all working toward shared outcomes. By defining CSFs clearly and quantitatively, leaders create a set of reference outcomes that reveal how these components interact to support (or jeopardize) strategic goals. When CSFs are mapped to workflows, IT assets, human roles, and third-party services, they form a "system map" that reflects real-world dependencies and feedback loops—key principles of systems thinking. This approach shifts decision-making from siloed optimization to enterprise-wide risk trade-offs. For instance, instead of improving latency in isolation, systems thinking encourages analysis of how that change affects data integrity, regulatory compliance, or staff workload. Ultimately, CSFs act as a systems-thinking tool by highlighting how local actions ripple across the organization's ecosystem, ensuring all interventions are measured by their contribution to sustained business value and resilience.

Clarify strategic goals and critical success factors (CSFs) - Crafting a systems-thinking cyber-aware ERM program begins with an almost forensic unpacking of corporate strategy into explicit, measurable critical-success factors (CSFs), because without that granularity every other cyber-risk conversation dissolves into abstractions. The work starts at the board table, where directors customarily voice ambitions—"gain three percentage points of market share," "preserve franchise value across cycles," "remain the safest counter-party in the industry"—yet those aspirations, however stirring, are abstract to engineers, operators, risk managers, and threat-intelligence analysts until they are rewritten as outcome-based sentences that bind technology performance, client experience, capital-markets confidence, and statutory duty into a single metric. Consider the declarative statement "Provide continuous, sub-100-microsecond trade matching for every product in every primary venue, with fewer than five minutes of unplanned downtime per calendar quarter." That single line expresses the institution's value proposition to clients, its operational-resilience obligation under SEC Regulation SCI, its exposure to the SEC's Cybersecurity Governance Rule, and its implied promise to shareholders that cyber disruption will not erode earnings. Once articulated, such a CSF becomes the "north star" against which every control, architectural decision, staffing plan, and incident-response dollar can be stress-tested; a line item in a budget request that cannot be traced to at least one CSF is immediately suspect, and a proposed feature whose time-to-market metric erodes the CSF's latency ceiling is swiftly escalated to a risk-appetite discussion.

In mature institutions, the translation process is neither ad-hoc nor anecdotal: it follows a workshop methodology referenced in the FDIC's 2024 Report on Cybersecurity

and Financial-System Resilience, which recommends a facilitated, cross-disciplinary "critical-service mapping" session. During that session, senior product owners, enterprise architects, site-reliability engineers, security architects, operations chiefs, legal counsel, and regulatory-affairs officers gather in a single room—physical or virtual—and walk revenue stream by revenue stream, settlement obligation by settlement obligation, brand promise by brand promise. For each line of business, they ask four canonical questions: (1) What outcome does the market pay us for? (2) What performance, confidentiality, integrity, and availability thresholds must be true for that outcome to remain unimpaired? (3) Which people, processes, technology assets, data flows, and external dependencies create or support that outcome? (4) What recovery behavior—expressed as RPO, RTO, maximum tolerable outage, and error-rate ceilings—defines "acceptable pain" versus "existential crisis" if an asset fails? The answers are documented in a "CSF register," a living catalogue whose rows align outcomes to key performance indicators (KPIs): latency ceilings, throughput floors, jitter envelopes, transaction-error boundaries, data-quality tolerances, aggregate limit-utilization thresholds, service-level objectives for upstream providers, and regulatory or contractual time-to-notify obligations. The register is stored in a version-controlled repository and made discoverable through the same self-service catalogue that developers consult for API specifications; each CSF record is tagged with business owner, risk-owner, regulatory citation, and downstream dashboards that expose real-time telemetry.

This register is not a dusty spreadsheet: it is wired into the firm's DevSecOps pipelines so that any pull request modifying a micro-service, database schema, or

infrastructure-as-code template triggers an automated policy-as-code gate using tools such as Open Policy Agent or HashiCorp Sentinel. If the proposed change risks violating the CSF's quantitative threshold—say, by increasing end-to-end message-processing latency 5 % beyond the 100-microsecond ceiling—the pipeline fails and requires explicit risk-owner sign-off or architectural redesign. Such automation embodies the SEC rule's edict that boards must disclose "processes for assessing, identifying, and managing material cybersecurity risks", because it shows a measurable, enforced workflow from code commit to board-level objective.

With measurable CSFs in place, risk-appetite statements gain teeth. Instead of vapid language — "management has low tolerance for cyber outages" — the board can promulgate quantified edicts: "The firm will not accept any risk scenario that jeopardizes CSF-01 (24×7 trade execution) without confirmed active-active fail-over in under 60 seconds, and will not tolerate client order-loss probability exceeding ten-in-a-million." The CRO then loads those thresholds into a Monte-Carlo engine that sits atop the dependency graph, producing loss-exceedance curves comparable to Value-at-Risk or Expected Shortfall portfolios.

Threat-intelligence teams leverage the CSF register as a triage lens. Every indicator of compromise (IOC) is mapped to the CSF it threatens: a Log4Shell exploit targeting an order-entry API raises CSF-01 to red within seconds, whereas phishing attempts against HR portals may stay amber unless and until lateral movement crosses into a CSF's dependency set. This practice example in its annual Operational-Resilience is radically more effective than first-come, first-serve alert queues because it aligns detection and

response with enterprise value. Likewise, vulnerability-management workflows adopt "value-at-stake scoring": CVSS 8.2 on a CSF-bound host outranks CVSS 9.8 on a non-critical kiosk. Analytic hierarchy processes encode subjective board value and regulatory fines into weights; the result is a backlog ordered not by raw severity but by CSF-normalized business impact.

The clarifying power of explicit CSFs surfaces organizational tensions early—tensions that might otherwise explode only in crisis. Product management's zeal to push weekly low-latency order-type enhancements, for instance, runs head-long into platform-stability engineers' warnings that each incremental change increases complexity and tail-risk. By measuring both objectives against CSF latency and error-rate budgets, leadership can negotiate trade-offs transparently: "We will permit two major feature deployments per quarter, provided pre-production load-testing demonstrates 99.999 % message-processing success at 90 % projected peak volume; otherwise, deployment is deferred or the CSF threshold is formally revised and the SEC is notified of changed risk posture." Every compromise is documented as a risk-appetite exception in the enterprise risk register (ERR); the entry includes CSF linkage, residual-risk delta, remedial roadmap, and expected date of restitution. This audit trail is invaluable when regulators perform horizontal reviews—like the SEC's focus on seeking clarity on how boards integrate cyber oversight into enterprise strategy, which can trigger enforcement against companies whose disclosures did not match internal governance artifacts.

The CSF framework also catalyzes more sophisticated capital-allocation conversations. Because each CSF references dollar-denominated revenue streams and

quantifies potential loss durations, CFOs can compute risk-adjusted return on resilience investment (RaRRI). If upgrading WAN acceleration shaves 10 microseconds off round-trip latency, thereby decreasing trade-slippage and increasing average daily volume, that uplift can be compared directly to the amortized hardware cost; similarly, a second hot-standby data-center that reduces RTO from five minutes to thirty seconds can be benchmarked against avoided penalty fees. Value-based storytelling turns cybersecurity from a cost center into a strategic differentiator: investor-relations decks can showcase audited uptime, latency, and recovery metrics as proof points for liquidity providers selecting execution venues

CSFs become the scaffold for incident-response playbooks, too. Red-team operators script attacks that aim to breach specific CSF thresholds; blue-teams practice containment maneuvers that restore metrics inside tolerance before the “material outage” reporting clock starts. Runbooks list decision trees keyed to CSF deltas: if average latency is > 85 microseconds but < 95 microseconds for more than ten seconds, reroute 20 % order flow to secondary region; if > 100 microseconds, declare SEV-1, fail over in 30 seconds, and alert central crisis management command and control team. Post-mortem root-cause analysis overlays time-series telemetry on CSF limits: investigators can see the exact millisecond latency pierced 100 μs, the packet-sequence that choked, the micro-service which triggered the cascading slowdown. Because the CSF threshold is regulatory as much as commercial, the same chart forms the backbone of the Form 8-K cyber-incident disclosure. Legal teams appreciate the reduction in subjective narrative; regulators appreciate the quantitative granularity; insurers appreciate the actuarial clarity; and

shareholders appreciate the unambiguous evidence that management grasps how cyber events map to enterprise value.

- CSF-anchored proactive testing extends into human-centric and third-party risk domains. People: The CSF register includes minimal staffing matrices—how many Tier-1 SREs must be awake and logged in to manage load spike? If shift swaps or pandemic absenteeism drop below that figure, the system's human availability threshold is breached, flagged in the enterprise GRC platform, and escalated to HR and business-continuity leads. Minimum staffing cumulative requirements can be clearly identified to support critical systems supporting critical business to achieve critical success factors.
- Process: Batch settlement cycles that reconcile intraday positions to clearing-house collateral requirements have error-rate tolerances; if exception queues exceed 200 trades after 15 minutes, CSF-04 ("timely settlement finality") is threatened, and fail-over to manual contingency procedures kicks in.
- Technology: Technology turns lofty ambitions into quantifiable, enforceable commitments by translating each critical-success factor into real-time data points that engineers can instrument, executives can monitor, and regulators can audit. Modern observability stacks, CI/CD pipelines, and policy-as-code engines embed latency ceilings, error-rate thresholds, and recovery-time targets directly in the software that powers the business, ensuring every deployment is automatically validated against strategic objectives. Dependency-mapping tools expose how applications, cloud services, and third-party APIs underpin each CSF, so leadership can see precisely where a cyber fault would erode value. Data analytics then convert raw telemetry into board-level dashboards, allowing risk

appetite to be set and adjusted on evidence rather than intuition. In short, technology supplies the instrumentation, automation, and visibility that make strategic goals measurable, enforceable, and continuously aligned with enterprise value.

Integrating CSFs into everyday culture means embedding them in performance reviews. Developers are measured not only on story-points delivered but on whether their commits produce latency, CPU, or error-rate deltas that threaten CSFs. SRE bonuses include a "mean time within CSF envelope" component; risk-officers gain incentive pay for cross-functional tabletop exercises that validate CSF scenarios. The CISO's scorecard shows not only phishing-click rates but proportion of CSF-linked hosts meeting patch SLA. There must be strong collaboration across the enterprise, "front-line, second-line, and third-line functions must share accountability for resilience" , anchoring evaluations to CSFs dismantles siloed blame cultures and reduces mean-time-to-recover by clarifying priorities.

Even external communications benefit. Investor-relations presentations no longer tout generic "99 % uptime" but showcase audited CSF performance: "During Q3, the average round-trip order latency for equity products remained at 83 µs (versus our CSF ceiling of 100 µs), and unplanned downtime totaled 61 seconds, well below the quarterly limit of 300 seconds." Analysts can translate numbers directly into revenue forecasts.

Finally, CSFs enable genuine systemic-risk contribution. ISACs and public-private taskforces exchange "CSF-aligned disruption scenarios" rather than generic incident feeds. Regulators aggregate anonymized CSF breach data to model sector-wide contagion: if the three largest equity venues share a common DNS provider, regulators can pre-

emptively coordinate fail-over drills. Such collective action inches the industry toward a systemic-resilience model akin to capital-adequacy stress tests.

Thus, a single meticulous step—translating board ambition into explicit, quantified, continuously governed CSFs—spawns a cascade of value: automated guardrails in software pipelines; quantitative risk-appetite statements coherent with capital planning; threat-intelligence triage rooted in enterprise value; negotiation frameworks that balance innovation with stability; incident-response runbooks that map actions to dollars saved; resilience investments whose ROI can be priced alongside trading strategies; credible regulatory disclosures that dodge enforcement; cultural incentives that unite first-, second-, and third-line functions; investor narratives that back earnings stability with empirical data; and sector-wide intelligence that upgrades from indicator-sharing to dependency-map exchange. By the time something as dramatic as the CrowdStrike Windows update meltdown occurs, institutions with mature CSF regimes can quantify exposure and re-route volume before headlines hit the wires. Cybersecurity, once an opaque insurance policy, becomes a transparent, value-accretive, strategy-aligned differentiator, fulfilling the intent of governance to be grounded in measurable, board-owned, publicly reportable commitments. Ultimately, explicit CSFs stitch together technology, operations, finance, and compliance into a single, continuously measured fabric of resilience, ensuring that the next decade of market-structure evolution happens atop a foundation that investors, regulators, and—crucially—customers can trust.

- Map business processes to supporting systems - With CSFs locked, institutions must expose the “digital plumbing” that actually delivers those outcomes by decomposing

each critical business process into machine-readable and human-actionable steps. Using tools such as BPMN or other workflow tools, analysts trace end-to-end process steps—order capture, order routing, trade matching, settlement confirmation, client reporting—and annotate each activity with the precise application, micro-service, database, network segment, cloud subscription, or third-party API that performs the work. This lineage view accomplishes two governance miracles. First, it replaces static asset inventories—often forgotten SharePoint lists—with a dynamic dependency graph showing exactly where a cyber-fault will interrupt value delivery. If the FIX gateway cluster fails, orders never reach the matching engine, instantly threatening the "continuous, sub-100-microsecond execution" CSF. Operations no longer debate whether a component matters; the map demonstrates the causal chain in black and white. Second, the exercise surfaces non-obvious common-mode dependencies such as shared DNS providers, certificate-authority endpoints, or message-broker clusters that multiple processes silently rely on. These shared services often represent systemic single points of failure yet remain invisible in siloed risk registers. Capturing them allows the institution to run blast-radius simulations that quantify just how many revenue lines collapse if, say, the cloud message-broker region goes dark. The mapping process is not a one-off project but rather embedded into CI/CD pipelines and configuration-management databases. Every time a DevSecOps pipeline deploys a new micro-service, hooks update the dependency graph, ensuring ERM views stay in lock-step with production reality rather than last quarter's topology slide. Crucially, the same map feeds incident response: when an alert fires, responders can click a node, see upstream/downstream CSFs, and choose containment strategies that minimize business

impact rather than arbitrarily isolating servers. In short, dependency mapping converts abstract architecture diagrams into living risk artefacts that guide both strategic capital allocation and minute-to-minute crisis management.

- Document critical resources across People, Process, and Technology (PPT) - Systems thinking posits that technology is merely one strand in a socio-technical web, so a robust dependency graph must catalogue the human roles, procedural hand-offs, and vendor relationships that keep the technical stack humming. For each workflow step, analysts capture: the accountable owner, required skill sets, minimal staffing levels, on-call rosters, vendor SLAs, manual fallback procedures, and archived run-books. This holistic inventory surfaces single points of human failure—such as a lone database engineer who holds the institution's only deep expertise in replication tuning—which, in a cyber crisis, can delay recovery as surely as a corrupted storage array. Similarly, mapping manual contingencies reveals process brittleness: if a trade-match exception must be reconciled by a human within fifteen minutes to meet settlement windows, any cyber event that slows staff access to enterprise portals now has a quantifiable operational impact. Furthermore, regulators increasingly scrutinize "operational resilience," a concept that cannot be satisfied by patching servers alone. A PPT-inclusive map demonstrates organizational maturity by showing that the firm anticipates people and process failures alongside technology compromises. Finally, the inventory feeds board-level key-person-risk dashboards, ensuring the budget for knowledge-transfer and documentation is weighed with the same gravity as firewall upgrades. When done well, the PPT mapping converts cyber-risk

governance from an IT issue to an enterprise-wide responsibility shared by HR, procurement, and every operational function.

- Define success criteria for systems and operating environments - After mapping dependencies, the institution must encode what "good looks like" at each node in the system, creating success criteria that bridge tactical engineering metrics and strategic CSFs. For performance, criteria may specify maximum packet loss on market-data feeds, sustained CPU utilization thresholds for core matching engines, or median time-to-acknowledge on FIX sessions. For security, the criteria might demand validated encryption configurations, key-rotation periods, zero hard-coded secrets, and multi-factor authentication enforcement. For resilience, success could mean RPO = zero transactions lost and RTO $\leq$ 60 seconds for hot/hot cloud failover. Crucially, thresholds must be testable by instrumentation. Observability stacks (Prometheus, OpenTelemetry, Splunk) emit metrics compared to these thresholds in real-time; violations generate alerts that feed both SecOps and risk-governance dashboards. Embedding thresholds into CI/CD policy-as-code, via tools like Open Policy Agent or HashiCorp Sentinel, ensures infrastructure that violates success criteria never reaches production. Governance forums maintain a "success-criteria playbook," reviewed quarterly to reflect shifting threat landscapes and business expansions—say, launching a crypto-options product with more stringent latency demands. Codifying criteria also transforms control-assurance debates: instead of arguing whether a firewall rule is "good enough," assurance teams test the environment against objective thresholds and report empirical pass/fail results. This empirical chain finally allows advanced risk-quantification frameworks (e.g., FAIR, stochastic Petri nets) to run on

credible input data, producing loss exceedance curves CROs can overlay on capital-adequacy planning. Regulators appreciate the transparency: when examiners ask how management knows controls are effective, dashboards show live metrics versus thresholds, change-history logs, and automated rollback counts. Ultimately, success criteria operationalize the concept that meeting every local threshold mathematically guarantees global CSF attainment, turning theoretical systems-thinking into executable engineering guardrails.

- Evaluate architecture and document ecosystem-specific inherent risks - Armed with dependency graphs and success criteria, the firm next performs architecture risk-assessments that enumerate failure modes inherent to the design itself—weak encryption between micro-services, overly flat networks, region-locked cloud dependencies, hard-coded secrets in pipelines, or excessive reliance on a single authentication provider. Each finding is phrased as an inherent risk: the probable loss before any mitigations. Documenting risk at this layer serves two strategic feedback loops. Upstream, enterprise architects can compare alternative designs via risk-adjusted return analyses, turning security engineers from naysayers into quantitative business partners. The CFO can explicitly weigh capex for segmenting the network against probabilistic downtime costs—because the architecture risk register quantifies both. Downstream, control owners gain a baseline against which to measure residual risk; they avoid complacency that arises when green dashboards mask structural brittleness. The architecture review process typically employs threat-modelling frameworks (STRIDE,PASTA), scenario analyses aligned to MITRE ATT&CK techniques, and design-review checklists drawn from CIS Benchmarks.

Findings feed gamified red/blue-team exercises that validate exploitability. Importantly, inherent risk ratings incorporate systemic propagation vectors: a compromise in the message-broker cluster not only affects trade flow but may also leak risk-management data, potentially skewing VAR models and cascading into capital-allocation errors. Regulators increasingly mandate such systemic perspectives and the SEC's proposed SCI updates, making architecture-level documentation a compliance necessity. Finally, by contextualizing inherent risk inside the CSF framework, boards gain clarity on why certain modernization projects—say, re-platforming legacy COBOL or end of life components—cannot be deferred without breaching risk appetite.

- Embed every inherent risk in the formal risk register - To prevent fragmentation, each architecture-level finding migrates into a single enterprise risk register (ERR) where cyber, credit, market, and liquidity exposures live side by side. This unified ERR holds metadata tags: CSF impacted, regulatory domain, control-family alignment (ISO 27001 clause, NIST CSF sub-category), business owner, mitigation plan, due date, and residual risk target. Seamless integration is automated: when a DevSecOps pipeline flags a new CVE on the container image that hosts the order-routing API, a ticket triggers ERR-API updates so boards see the exposure within hours, not months. Housing cyber risks in the same ERR as financial-risk items forces balanced capital allocation discussions: will the company spend on market-data feed redundancy or on credit-risk hedging? The answer is driven by impact distributions plotted from ERR data rather than "gut feel." Moreover, unified visibility stops the turf wars that arise when IT keeps one register in ServiceNow, operations another in Excel, and audit a third in GRC tools. Audit committees demand "one

source of truth," and the ERR satisfies that requirement. Integration also accelerates regulatory submissions: when examiners ask for evidence that cyber threats are considered in ICAAP or CCAR stress tests, the firm simply exports the ERR slice showing scenario linkages. Finally, having cyber risks share a taxonomy with other risks enables advanced portfolio-style optimization: Monte Carlo engines can model cross-risk contagion to compute risk-adjusted RoRAC, guiding C-suite resource prioritization toward initiatives that maximize resilience ROI.

- Score each inherent risk for likelihood and impact - Quantification turns qualitative architecture critiques into numbers leadership can act on. Likelihood estimates blend threat-intelligence feeds (exploit frequency, adversary sophistication, industry-specific campaigns) with internal vulnerability telemetry (patch cadence, privilege sprawl, code-scanning results). Impact calculations mix direct losses (fraud, forensic costs, legal penalties) and systemic knock-ons such as liquidity shocks triggered by trading halts or capital drains. Firms may choose to deploy Bayesian networks, Monte Carlo simulations, or agent-based models to propagate probabilities across the dependency graph: if the market-data ingest fails, long/short books may diverge from real prices, increasing VaR. Such analytics reveal non-linear interactions—a DDoS increases latency, which in turn elevates credit exposure when hedges cannot be placed. Quantified scores feed heat-map dashboards that spotlight risks exceeding appetite, prompting mitigation or transfer decisions. They also tie to key-risk-indicator (KRI) thresholds; when attacker chatter spikes on dark-web forums, likelihood scores auto-adjust, changing risk ranks overnight. Translating numbers into economic capital lets CROs integrate cyber into scenario-analysis

frameworks ensuring cyber shocks are considered in capital-adequacy estimates. Externally, insurers increasingly require quantified data to price cyber-premiums; detailed likelihood-impact matrices can lower premiums by evidencing rigorous governance. Quantification thus closes the loop: cyber metrics hold their own next to market-risk Greeks and credit-risk, institutionalizing cyber as a first-order financial-risk driver, not an IT footnote.

- Explain dependencies so stakeholders grasp systemic cyber impacts - The last mile is communication: turning graphs and probability tables into intuitive narratives that prompt informed decisions. Visual dependency maps annotated with CSFs and Risk Register status become the centerpiece of quarterly board packs, where directors can zoom from 30,000-foot summaries—"Order routing depends on three cloud regions"—down to node-level metrics—"Region us-east-1 currently runs at 82 % capacity with RTO 45 seconds." Scenario storyboards walk executives through plausible attack chains: "A nation-state actor exploits the container-runtime CVE, pivots into the message-broker, disrupts market-data flow, causing price-discovery gaps, triggering trading halts, violating CSF #1, invoking Reg SCI escalation." Such narratives help non-technical leaders internalize cascading effects that raw logs cannot convey. Externally, appropriately sanitized dependency insights shared with ISACs foster sector-wide resilience; peers can coordinate patch cycles to avoid simultaneous outages. Internally, the same artefacts train new hires and incident-response teams, embedding systems thinking into the firm's DNA. Communication is two-way: feedback from real incidents—near misses, red-team drills—updates the dependency map, ensuring lessons learned feed forward. When a ransomware

incident hits a peer exchange, the map helps answer, “Could that happen here? Which CSFs would be at risk?” Regulators increasingly reward transparency; firms that can articulate dependencies and scenario impacts during supervisory reviews build credibility that translates into lighter supervisory friction. Ultimately, storytelling built on robust data turns systems-thinking from an academic ideal into lived corporate culture, ensuring every stakeholder, from coders to chairpersons, understands how their daily choices influence enterprise resilience.

- Interpretation of Key Findings - This study highlights how Critical Success Factors (CSFs) function as the structural backbone of a systems thinking-based cybersecurity ERM program. The findings show that when CSFs are explicitly defined, quantified, and operationalized, they transcend departmental boundaries to become enterprise-wide control points that align strategic goals with real-time operational decisions. The integration of CSFs into Application Development-Architecture-Sysops-DevSecOps pipelines, risk registers, incident response playbooks, and board reporting demonstrates the system-wide feedback loops envisioned by systems thinking.

  The use of tools such as dependency mapping, telemetry-fed observability stacks, and automated policy-as-code gates reveals a shift from reactive to anticipatory risk management. This suggests that CSFs are not only enablers of resilience but also instruments of strategic performance control.

- Link to Research Questions and Objectives - The primary objective of this research was to explore how systems thinking could be applied to govern cybersecurity risks through the lens of enterprise risk management. The study specifically aimed to identify

how CSFs support this integration. The results clearly address this goal: CSFs provide the measurable, dynamic anchors that translate abstract strategy into operational behavior, enabling a holistic cyber governance framework that meets both regulatory and performance expectations.

Comparison with Previous Studies - These findings support and extend prior literature on systems thinking in cyber risk. While earlier studies emphasized the interdependence of systems (Sterman, 2000; NIST IR 8286), this paper operationalizes that theory by embedding CSFs into real-world engineering and governance artifacts. Unlike traditional ERM models that treat cyber as an isolated domain, this CSF-centric approach echoes best practices emerging in regulatory guidance, such as those found in FDIC (2024) and SEC Regulation SCI.

- Implications:

1. For practitioners, CSFs provide a traceable, auditable bridge between strategy, controls, and capital planning. This can be achieved by considering the following implementation points.
    - CSF-to-Control Mapping Framework – Develop a documented methodology that explicitly links each Critical Success Factor (CSF) to specific cybersecurity controls, business processes, and risk owners.
    - Integrated Risk & Capital Planning Dashboard – Build dashboards that show CSF performance alongside risk exposure metrics and associated capital allocations, enabling traceability for both operational and strategic reviews.

- Audit-Ready Documentation – Maintain a central repository of evidence showing how CSFs influence control selection, investment priorities, and budget decisions, ensuring it meets internal audit and regulatory examination requirements.
- Governance Oversight Cycle – Incorporate CSF reviews into quarterly risk committee and board reporting to validate alignment with business strategy and update capital plans as needed.
- Scenario-Based Capital Stress Testing – Simulate scenarios where CSFs are stressed (e.g., loss of system availability) to assess capital adequacy and inform contingency funding plans.

2. For regulators, the approach demonstrates compliance with the SEC's and CFTC's expectations for documented, measurable cyber oversight. This can be achieved by considering the following implementation points.
    - Regulatory Mapping Matrix – Create a documented crosswalk aligning cybersecurity policies, procedures, and metrics with specific SEC and CFTC requirements (e.g., Reg SCI Matrix).
    - Measurable Oversight KPIs – Define quantitative and qualitative indicators (e.g., incident response times, vulnerability remediation rates) that can be regularly reported to demonstrate ongoing compliance.
    - Board and Committee Reporting Templates – Standardize formats for presenting cyber oversight evidence to governance bodies, ensuring traceability and readiness for regulatory review.

- Independent Assurance Reviews – Engage internal audit or third-party assessors to validate that oversight practices are effective, documented, and meet regulator expectations.
- Regulatory Scenario Exercises – Conduct table-top simulations of SEC/CFTC-reportable incidents to test readiness for timely, accurate disclosures.

3. For risk managers, CSFs enable better tailored risk assessment approach and automated exception tracking. This can be achieved by considering the following implementation points.
    - CSF-Driven Risk Assessment Templates – Design assessment tools that structure questions, scoring, and risk ratings directly around Critical Success Factors, ensuring relevance to business priorities.
    - Automated Exception Tracking System – Integrate risk assessments with a GRC (Governance, Risk, and Compliance) platform to automatically log, assign, and track exceptions against CSF-related controls.
    - Dynamic Risk Scoring Models – Use CSF performance metrics to adjust inherent and residual risk scores in real time, enabling more precise prioritization.
    - Exception Aging and Escalation Rules – Establish automated workflows that flag overdue exceptions and escalate them to appropriate governance bodies.

- Risk Heatmaps Linked to CSFs – Create visualizations showing where CSFs face the highest risk exposure, updated automatically from assessment and monitoring data.

4. For developers and engineers, the CSF framework embeds performance and compliance into deployment workflows via SDLC, CI/CD automation etc. This can be achieved by considering the following implementation points.
    - CSF-Integrated SDLC Checkpoints – Embed CSF-based security and compliance requirements into each phase of the Software Development Life Cycle, from design to deployment.
    - CI/CD Pipeline Compliance Gates – Configure automated checks in continuous integration/continuous deployment workflows to validate code against CSF-aligned security policies before release.
    - Infrastructure-as-Code (IaC) Policy Enforcement – Apply CSF-driven guardrails in IaC templates to ensure infrastructure deployments meet performance, resilience, and compliance standards.
    - Automated Test Suites – Develop test cases linked to CSF objectives (e.g., latency, availability, encryption) that run automatically during builds and deployments.
    - Developer Feedback Dashboards – Provide real-time CSF compliance and performance metrics to engineers, enabling proactive remediation before production release.

5. For executives and boards, the use of dashboards and dependency maps makes cyber risk intuitively navigable and strategically actionable. This can be achieved by considering the following implementation points.
    - Executive Cyber Risk Dashboards – Design high-level dashboards that translate technical risk metrics into business impact terms, using visual cues like traffic-light indicators.
    - Dependency Mapping Tools – Develop interactive maps linking critical business processes, technologies, and vendors to show where cyber risks could disrupt strategic objectives.
    - Scenario-Based Strategy Sessions – Use dependency maps to model "what-if" scenarios and inform contingency planning, capital allocation, and investment prioritization.
    - Board Education Programs – Conduct periodic briefings to build familiarity with dashboard indicators, dependency relationships, and their relevance to strategic decisions.
    - Decision-Trigger Thresholds – Define agreed-upon risk thresholds within dashboards that automatically prompt governance action when exceeded.

- Systems Thinking Context - CSFs are inherently systems thinking instruments. They define emergent properties (e.g., "sub-100µs latency with zero downtime") that rely on the interaction of many parts—infrastructure, applications, processes, people, and third-party vendors. The architecture described leverages feedback loops (e.g., CI/CD gates

blocking risky code), causal relationships (e.g., staffing gaps leading to process breakdown), and dynamic adaptation (e.g., incident scenarios refining telemetry thresholds). CSFs thus serve as the system's measurable heartbeat, aligning every subsystem to the overall mission.

- Limitations and Alternative Explanations - While comprehensive, this study's reliance on a theoretically mature implementation of CSFs (as seen in elite trading environments) may limit generalizability to less digitally advanced sectors. Smaller institutions may lack the observability infrastructure or cultural maturity to automate CSF enforcement via pipelines. Additionally, real-world application might be constrained by siloed data ownership, lack of cross-functional alignment, or limited tooling budgets.

An alternative explanation could be that strong cybersecurity performance results more from organizational culture or leadership commitment than from any specific CSF mechanism. However, the integration of CSFs into pipelines, dashboards, and risk appetite frameworks provides compelling evidence of causal alignment.

- Recommendations for Future Research - Future studies could expand on the following.
    - Conducting research to evaluate how CSF maturity evolves over time within an institution can provide valuable insights for governance and strategic planning. Such research enables ongoing trend analysis to determine whether CSF adoption is progressing, stagnating, or regressing, allowing for timely, targeted interventions. It can link CSF maturity growth to measurable business outcomes such as improved system uptime, faster

incident response, stronger regulatory compliance, and enhanced customer trust. Benchmarking capabilities can be developed to compare performance across business units internally and against peer institutions externally. This research also supports investment optimization by helping leadership assess whether spending on cyber capabilities delivers measurable gains in governance and resilience, while reinforcing regulatory confidence through a disciplined, measurable approach to cyber oversight. Potential research performers include internal audit and risk management teams conducting independent assessments, academic researchers developing longitudinal models, consulting and advisory firms comparing maturity trajectories across clients, industry associations such as FS-ISAC conducting aggregated sector-wide studies, and regulators or supervisory agencies assessing improvements in governance practices over multi-year periods.

- Comparing CSF frameworks across industries—such as financial exchanges, banks, and healthcare—can reveal how sector-specific priorities, regulatory requirements, and operational models shape the definition and application of Critical Success Factors. This research could highlight best practices that are transferable between sectors, as well as unique elements that must remain industry-specific due to compliance obligations, risk appetites, or threat landscapes. Cross-industry analysis can also identify gaps where certain sectors may be underemphasizing key CSFs, enabling targeted improvements and more robust resilience strategies. Findings could

inform regulators, industry bodies, and standard-setting organizations, fostering greater consistency and interoperability in cyber risk governance. Potential research performers include academic institutions conducting comparative studies, consulting firms with multi-sector client portfolios, industry associations facilitating cross-sector knowledge exchange, and regulatory agencies interested in harmonizing oversight approaches. Explore how AI and machine learning could further optimize CSF thresholds or predict deviations before they occur.

- Conducting case studies on how CSFs interact with regulatory reviews—such as horizontal enforcement actions by the SEC or CFTC—can provide practical insights into how well these frameworks perform under real-world scrutiny. Such research can reveal whether CSFs help institutions anticipate regulator focus areas, streamline evidence gathering, and demonstrate compliance during examinations or investigations. It can also identify patterns in how regulatory findings map to specific CSFs, highlighting strengths to preserve and weaknesses to address. These insights can improve alignment between business priorities, cyber governance, and regulatory expectations, ultimately reducing the risk of penalties or remediation mandates. Potential research performers include internal compliance and legal teams conducting post-review analyses, academic researchers studying enforcement trends, consulting firms specializing in regulatory readiness,

and industry associations aggregating anonymized lessons learned across member institutions.

5.2.1 Conclusion

The findings demonstrate that CSFs, when developed through systems thinking, serve as both strategic alignment tools and operational enforcement mechanisms. By turning abstract ambitions into observable metrics, CSFs enable firms to govern cyber risk with precision, adaptiveness, and transparency. This discussion confirms that the integration of cyber governance into ERM is not only feasible but fundamentally enhanced by systems thinking. Institutions that adopt this approach are better positioned to demonstrate resilience, accountability, and long-term stakeholder value.

5.3 Discussion of Research Question Two

Discussion: Cybersecurity Governance Models and Disclosure Frameworks in Financial Institutions

In light of increasing threat velocity and regulatory scrutiny, financial institutions are under intensifying pressure to mature their cybersecurity governance models and embed disclosure frameworks that enable real-time responsiveness to cyber threats. Traditional models that placed cybersecurity exclusively under the IT or compliance function have proven insufficient for today's dynamic threat landscape. Instead, a systems thinking approach—one that recognizes the interdependence of people, processes, technologies, and third parties—is gaining traction. Recent incidents such as the CrowdStrike Falcon Sensor outage (CrowdStrike, 2024), the ION ransomware attack (Assured, 2023), and sophisticated social engineering attempts targeting Coinbase, Binance, and Kraken

(CoinDesk, 2025; Fox Business, 2025) reveal the operational, reputational, and financial consequences of fragmented or reactive governance. These events, when examined against the board-level risk governance practices adopted by exchanges such as Cboe Global Markets (2024), Nasdaq (2023), and Intercontinental Exchange (2023), offer clear guidance on how financial institutions can establish a holistic, board-aligned cyber governance architecture.

Cboe Global Markets' Risk Committee Charter outlines a governance model where the committee assists the board in overseeing the firm's enterprise risk management framework, including cybersecurity, information security, operational risk, and business continuity (Cboe Global Markets, 2024). This structure formalizes cybersecurity as an integrated enterprise risk rather than a separate IT risk. Similarly, Nasdaq's Risk Committee Charter states that its oversight responsibilities include reviewing risk management policies and practices related to cybersecurity, vendor risks, and crisis management (Nasdaq, 2023). The Intercontinental Exchange (ICE) goes further, explicitly assigning the board-level Risk Committee the duty of overseeing the cybersecurity risk posture, approving risk thresholds, and reviewing incident response plans (Intercontinental Exchange, 2023). These governance charters align with SEC requirements—particularly post-2023 amendments—which mandate disclosure of how cybersecurity is governed at the board and management levels, and timely reporting of material cyber incidents under Form 8-K Item 1.05.

The CrowdStrike Falcon Sensor outage in July 2024, which resulted in widespread system crashes due to a faulty software update, demonstrated the systemic nature of vendor

risk. Many institutions suffered outages not due to malicious attacks but because of a breakdown in the reliability of a single endpoint security provider (CrowdStrike, 2024). This incident underscores the importance of board-level committees maintaining not just visibility into, but active governance over, vendor dependencies. Third-party risk management, as emphasized in ICE's charter, must be more than an annual audit requirement—it must include real-time dashboard visibility into vendor service-level performance, incident escalation protocols, and regulatory reporting accountability. In this case, many institutions failed to assess whether such a vendor issue constituted a material event under SEC guidelines, leading to inconsistencies in disclosure and reputational damage. A systems thinking approach highlights that third-party technology risks are tightly coupled with operational resilience and therefore must be directly mapped to critical success factors (CSFs) such as platform uptime, data integrity, and trade execution speed.

The ION ransomware attack in 2023 exposed a similar vulnerability—this time through dependency on a vendor that supports the derivatives trading infrastructure. The ransomware incident caused several trading desks to resort to manual processes, impacting clearing, settlement, and reporting (Assured, 2023). The case emphasized the need for tabletop exercises that incorporate third-party scenarios, a governance best practice recommended in Nasdaq's risk oversight framework. When third-party risks are not simulated in board-level incident planning, institutions may underestimate the systemic impact of a single vendor breach. Furthermore, the lack of transparency around materiality assessments delayed Form 8-K filings for institutions that were unsure whether indirect impacts—like delayed settlement—met the materiality threshold. Under the SEC's

materiality framework, as clarified in 2023, the source of the breach (internal or third-party) is irrelevant; what matters is the impact on the registrant's operations, financial condition, or reputation. Therefore, effective governance models must ensure that incident response teams—comprising Legal, Compliance, Risk, and InfoSec—are equipped to make materiality assessments and disclosure decisions within four business days.

Board-level training and scenario-based discussions—mandated in all three charters (Cboe, Nasdaq, ICE)—become particularly salient in such situations. These sessions must go beyond generic threat landscapes to include quantified impact analyses. For instance, the Coinbase incident, which revealed that a successful breach could cost up to $400 million, makes a compelling case for cyber risk quantification (Fox Business, 2025). Institutions must simulate the financial, legal, and operational implications of such losses during board training. Governance dashboards should include metrics like cyber value-at-risk (VaR), insurance coverage gaps, and regulatory fine estimates. Without quantification, board committees may fail to grasp the urgency of required control investments or the full implications of disclosure.

The thwarted social engineering attempts on Binance and Kraken in 2025 present a different lesson—namely, the need to govern the human layer of cybersecurity (CoinDesk, 2025). These attacks targeted employees through impersonation schemes and phishing, highlighting that even the most secure technology stack can be bypassed via cognitive exploits. The institutions that successfully fended off the attacks did so because of continuous employee training and immediate escalation protocols, governed not just by IT teams but validated through board-mandated cyber awareness KPIs. ICE's risk oversight

model includes regular review of incident reporting and employee awareness campaigns, practices that clearly contributed to Binance and Kraken's resilience. Institutions must mandate cyber KPIs such as phishing response rates, MFA enforcement percentages, and user access anomalies—data that should be integrated into ERM dashboards and reviewed by Risk Committees.

Another governance dimension surfaced during the ION and CrowdStrike events is the need for change management governance. In both cases, unanticipated technology changes (a ransomware attack in one, a faulty update in the other) led to material business impacts. Nasdaq's committee charter requires oversight of "technology risk" and mandates regular updates on technology transitions and outages (Nasdaq, 2023). A systems perspective sees change management as a node that connects multiple subsystems—cybersecurity, compliance, service availability, and vendor management. Effective governance therefore must include controls that validate the rollback capabilities of vendors, ensure redundancy, and verify testing practices before updates go live across production environments. Risk Committees should require quarterly reports on major configuration changes, firmware updates, and cloud migrations—each of which could become a source of vulnerability.

The SEC's disclosure framework adds another layer of complexity—and opportunity. Form 10-K now requires detailed narrative on cybersecurity governance, board oversight, and management roles in cyber risk (SEC, 2023). Form 8-K mandates timely public disclosure of material cybersecurity incidents within four business days. These requirements have reoriented internal governance, compelling institutions to adopt

what one CISO described as an “internal countdown clock.” The timing forces alignment between operational metrics, legal thresholds, and communication strategies. As ICE’s charter indicates, Risk Committees must oversee not just incident response plans, but also review the process by which materiality is determined and disclosures are drafted (Intercontinental Exchange, 2023). This requires tight coordination between Legal, Risk, InfoSec, and Investor Relations functions. From a systems thinking standpoint, regulatory disclosure acts as an exogenous feedback loop, enforcing accountability and transparency while driving internal behavioral change.

In addition to structure and reporting, culture remains a cornerstone of governance effectiveness. Institutions that tie cybersecurity goals to executive KPIs—such as requiring business unit leaders to meet vulnerability remediation SLAs or including cyber compliance in annual reviews—reported stronger engagement and fewer governance gaps. Cboe’s charter emphasizes that management is responsible for “embedding risk ownership into business processes,” a principle that aligns with the cultural dimension of systems thinking (Cboe Global Markets, 2024). Tabletop exercises that simulate SEC disclosure timelines, ransomware negotiations, or operational continuity under attack scenarios reinforce this culture and provide the Risk Committee with insight into organizational preparedness. Governance must also monitor the speed of response, a variable that’s increasingly being scrutinized by regulators and investors alike.

Finally, cross-pollination between governance domains—e.g., integrating cybersecurity into strategic planning and product development—emerged as a leading indicator of governance maturity. CISO involvement in cloud migration, M&A due

diligence, and digital asset initiatives reflects a "shift left" in cyber governance. ICE's charter explicitly requires the Risk Committee to review cybersecurity as part of "new and emerging risks," suggesting an anticipatory, rather than reactive, posture (Intercontinental Exchange, 2023). A systems approach mandates that cyber risk is not a downstream audit concern but an upstream design input, embedded early in project lifecycles. By treating cyber as a strategic enabler—rather than a compliance blocker—institutions unlock innovation while preserving security.

In conclusion, recent cybersecurity incidents reinforce the need for financial institutions to adopt governance models that are integrated, dynamic, and anchored in systems thinking. The structures outlined in the risk charters of Cboe, Nasdaq, and ICE offer valuable blueprints: establish empowered Risk Committees, integrate cyber metrics into ERM dashboards, enforce third-party oversight, and embed incident response simulations into governance routines. Disclosure frameworks mandated by the SEC introduce regulatory feedback loops that, if properly harnessed, elevate cyber risk governance to the board level. Real-world breaches—from CrowdStrike's outage to ION's ransomware and the thwarted attacks on crypto exchanges—illustrate that cybersecurity governance is not a static compliance artifact, but a strategic function tied to enterprise resilience. Financial institutions that embed cyber governance into their DNA—through culture, structure, metrics, and training—will not only meet regulatory expectations but also secure competitive advantage in a risk-saturated digital economy.

Implications - The move toward integrated, systems thinking–based cybersecurity governance has far-reaching implications for financial institutions. Incidents like the

CrowdStrike Falcon Sensor outage and the ION ransomware attack demonstrate that vendor dependencies, once considered operational details, now represent systemic risk vectors with the potential to disrupt entire market segments. These cases revealed that governance models relying solely on annual vendor risk reviews and static contract clauses are insufficient for a real-time threat environment. The practical implication is that institutions must embed vendor oversight into continuous monitoring programs with service-level dashboards, automated alerting, and clearly defined escalation thresholds tied to regulatory disclosure triggers. Without this, firms risk inconsistent determinations of materiality, delayed Form 8-K filings, and erosion of investor confidence when public narratives diverge from actual impacts.

Board-level engagement in cybersecurity oversight has shifted from a best practice to a regulatory requirement under the SEC's 2023 amendments, which explicitly link governance disclosures to board responsibilities. The implication is that boards can no longer delegate cybersecurity entirely to operational functions without maintaining active, informed oversight. This may require structural changes such as empowering Risk Committees with explicit cyber mandates, integrating cyber value-at-risk (VaR) and other quantifiable metrics into ERM dashboards, and mandating regular scenario-based tabletop exercises that include third-party breach simulations. Without these mechanisms, boards may lack the situational awareness and analytical grounding to make rapid capital allocation, operational continuity, and disclosure decisions within the four-business-day SEC window—leaving institutions exposed to both regulatory sanctions and reputational damage.

The governance challenges are not purely structural; they are cultural. A systems perspective underscores that the most mature governance models tie cyber accountability to executive and business unit KPIs, ensuring that risk ownership is embedded into day-to-day decision-making. This includes governing the human layer of security—where social engineering attacks, such as those attempted on Binance and Kraken, remain a persistent threat—through continuous training, phishing simulation metrics, and mandatory escalation protocols. It also extends to change management, where oversight of major technology changes, cloud migrations, or software updates must be embedded into board reporting cycles. Without a culture that reinforces cyber considerations in every operational and strategic decision, even the most sophisticated governance structures may fail in execution under real-world pressure.

Addressing these implications requires both immediate governance enhancements and a sustained research agenda. Comparative studies of Critical Success Factor (CSF) frameworks across sectors such as exchanges, banks, and healthcare could identify transferable resilience practices and highlight sector-specific vulnerabilities. Longitudinal research tracking CSF maturity within institutions could link governance evolution to measurable improvements in incident response times, regulatory compliance rates, and operational continuity. This work could be carried out by academic institutions developing governance maturity models, industry associations like FS-ISAC conducting anonymized benchmarking, consulting and advisory firms synthesizing cross-client data, and regulatory agencies assessing systemic readiness. By combining real-time governance reform with ongoing multi-stakeholder research, financial institutions can transform cybersecurity

governance from a reactive compliance activity into a dynamic, strategic function that strengthens both regulatory alignment and competitive positioning.

Systems Thinking Context:

Interdependencies are explicitly recognized - The governance model links board oversight, vendor performance, operational resilience, and regulatory disclosure into a single feedback loop. For example, a vendor outage (CrowdStrike) triggers operational impacts, which require coordinated action across Risk, Legal, Compliance, and IT, ultimately feeding into board decisions and public disclosures.

Feedback loops drive continuous adaptation - Regulatory disclosure requirements act as an exogenous feedback loop, forcing alignment between internal metrics, incident assessment processes, and external communication strategies. Internally, CSF maturity tracking and ERM dashboards create endogenous feedback loops that inform capital planning, risk prioritization, and cultural reinforcement.

Leverage points are identified for intervention - The recommendations focus on high-impact governance nodes—board committee mandates, vendor oversight dashboards, change management controls, and executive KPIs—that can shift system behavior toward resilience.

Cultural and structural elements are integrated - Systems thinking acknowledges that resilience is not achieved through technology alone; culture (shared accountability, training, escalation protocols) and structure (Risk Committees, reporting frameworks) are co-dependent components that must evolve together.

Adaptation across boundaries is encouraged - Cross-industry research and CSF benchmarking introduce learning loops from outside the institution's immediate system, reducing insular thinking and enhancing adaptive capacity.

Limitations and Alternative Explanations - While the analysis underscores the value of systems thinking–based cybersecurity governance, several limitations must be acknowledged. First, the case examples—such as the CrowdStrike outage, ION ransomware attack, and crypto exchange social engineering attempts—are inherently event-specific and may not fully represent the broader range of cyber incidents affecting financial institutions. Outcomes in these cases could be influenced by unique organizational factors, including existing risk culture, prior incident experience, or specific vendor relationships, which limit the generalizability of findings. Second, the governance models examined in the charters of Cboe, Nasdaq, and ICE are self-reported frameworks that reflect intended structures rather than guaranteed operational performance; real-world execution may deviate due to resource constraints, competing priorities, or organizational politics. Third, while SEC disclosure rules create a formal compliance framework, actual board and management behavior may be shaped more by internal risk appetites, market pressures, or leadership turnover than by regulatory mandates alone.

Alternative explanations must also be considered when interpreting the observed resilience and governance performance in certain institutions. For example, successful mitigation of the Binance and Kraken social engineering attempts may have been driven as much by strong individual employee vigilance as by institutional governance structures or KPIs. Similarly, relatively swift recovery from vendor-related disruptions may reflect pre-

existing technological redundancies or vendor-specific service capabilities rather than deliberate board-level oversight. Additionally, cross-institutional differences in capital resources, cyber insurance coverage, and tolerance for operational downtime may influence both governance investment decisions and disclosure strategies, independent of systems thinking maturity. Finally, while the proposed research agenda—such as CSF benchmarking and longitudinal maturity tracking—promises actionable insights, it is constrained by challenges in data availability, confidentiality, and standardization. Many institutions may be unwilling to share detailed governance and incident performance data, limiting the feasibility of comprehensive sector-wide studies. Furthermore, the dynamic nature of cyber threats means that governance best practices may evolve faster than longitudinal studies can capture, requiring adaptive research designs and continuous updates to maintain relevance.

Recommendations for Future Research - Future research should focus on tracking the longitudinal evolution of Critical Success Factor (CSF) maturity within financial institutions to better understand how governance capabilities develop over time and which interventions produce measurable gains in resilience. Such studies should examine correlations between CSF maturity and key performance indicators, including incident response times, regulatory compliance rates, operational continuity metrics, and capital allocation patterns. This evidence would help identify which governance investments yield the greatest return in reducing systemic cyber risk.

Comparative, cross-sector studies are also essential, evaluating how CSFs are defined, monitored, and governed in industries beyond financial services, such as

healthcare, energy, and transportation. This type of research could uncover sector-specific strengths and vulnerabilities, highlight transferable best practices, and reveal areas where financial institutions may lag behind other critical infrastructure sectors. In addition, further inquiry should examine the role of board engagement, assessing how governance structures, cyber risk quantification practices, and oversight processes influence the timeliness and accuracy of SEC-mandated disclosures.

Targeted case study research could explore how CSFs interact with regulatory reviews and enforcement actions, including horizontal examinations or coordinated initiatives by the SEC and CFTC. These studies could clarify how governance frameworks affect the speed, accuracy, and consistency of materiality assessments and public disclosures under strict reporting deadlines. Another promising avenue is evaluating the integration of human-layer risk governance—such as phishing response rates, multi-factor authentication (MFA) enforcement, and employee awareness training—into enterprise risk dashboards, and measuring their impact on breach prevention.

- Additional research can be performed by the following:
    - Academic Institutions and Research Centers – To develop validated maturity models, comparative analyses, and longitudinal studies with peer-reviewed rigor.
    - Industry Associations (e.g., FS-ISAC, ISDA) – To conduct anonymized benchmarking and cross-member surveys on governance practices and CSF adoption.

- Regulatory and Supervisory Agencies (e.g., SEC, CFTC, Federal Reserve) – To assess sector-wide readiness, identify systemic weaknesses, and inform policy development.
- Consulting and Advisory Firms – To leverage multi-client data for practical, implementation-focused studies that bridge theory and execution.

By distributing these research responsibilities across academic, industry, regulatory, and commercial stakeholders, the sector can generate both academically rigorous insights and operationally relevant findings, ensuring that cybersecurity governance models evolve in step with regulatory expectations and an ever-changing threat landscape.

5.3.1 Conclusion

In conclusion, advancing cybersecurity governance in financial institutions requires a coordinated, systems thinking–driven approach that integrates structural oversight, cultural accountability, and continuous learning. By treating Critical Success Factors as dynamic connectors between strategic objectives, operational controls, and regulatory compliance, institutions can better anticipate, withstand, and adapt to evolving threats. The recommended research agenda—spanning longitudinal maturity tracking, cross-sector comparisons, regulatory case studies, and human-layer risk analysis—offers a pathway to deepen understanding of what drives measurable resilience. Engaging a diverse set of stakeholders, from academic institutions and industry associations to regulators, consultants, and technology providers, will ensure that insights are both rigorous and practical. Ultimately, embedding these findings into governance practice will not only

strengthen compliance with SEC and CFTC expectations but also position institutions to sustain trust, operational continuity, and competitive advantage in an increasingly complex cyber risk environment.

REFERENCES:

Abkowitz, M. D. (2008). Operational risk management: A case study approach to effective planning and response. John Wiley and Sons.

Acharyya, M., and Brady, C. (2014). Designing an enterprise risk management curriculum for business studies: insights from a pilot program. Risk Management and Insurance Review, 17(1), 113–136.

Aebi, V., Sabato, G., and Schmid, M. (2012). Risk management, corporate governance, and bank performance in the financial crisis. Journal of Banking and Finance, 36(12), 3213–3226.

Agarwal, R., and Kallapur, S. (2018). Cognitive risk culture and advanced roles of actors in risk governance: a case study. The Journal of Risk Finance, 19(4), 327–342.

Aggarwal, R., Ferrell, A., and Katz, J. G. (2007). US securities regulation in a world of global exchanges. Exchanges: Challenges and Implications, Euromoney.

Agustina, L., and Baroroh, N. (2016). The relationship between Enterprise Risk Management (ERM) and firm value mediated through the financial performance. Review of Integrative Business and Economics Research, 5(1), 128.

Al-Alawi, A. I., and Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. Journal of Xidian University, 14(7), 1523–1536.

Al-Khadash, H. A., Jireis, J. R., and Embassy-Jordan, U. S. (2017). COSO enterprise risk management implementation in Jordanian commercial banks and its impact on financial performance.

Al-Saggaf, Y., and Islam, M. Z. (2015). Data mining and privacy of social network sites' users: Implications of the data mining problem. Science and Engineering Ethics, 21, 941–966.

Alawattegama, K. K. (2018). The impact of enterprise risk management on firm performance: Evidence from Sri Lankan banking and finance industry. International Journal of Business and Management, 13(1), 225–237.

Althonayan, A., and Andronache, A. (2019). Resiliency under strategic foresight: The effects of cybersecurity management and enterprise risk management alignment. 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), 1–9.

Arcuri, M. C., Brogi, M., and Gandolfi, G. (2018). The effect of cyber-attacks on stock returns. Corporate Ownership and Control, 15(2), 70–83.

Arena, M., Arnaboldi, M., and Azzone, G. (2010). The organizational dynamics of enterprise risk management. Accounting, Organizations and Society, 35(7), 659–675.

Assured. (2023). Unlocking the truth: An inside look at the ION ransomware attack. https://assured.co.uk/2023/unlocking-the-truth-an-inside-look-at-the-ion-ransomware-attack/

Azizi, N., and Hashim, K. (2008). Enterprise level it risk management. Proceedings of the 8th WSEAS International Conference on Applied Computer Science (ACS'08).

Bayuk, J. (2005). Stepping through the IS audit, a guide for information systems managers. Information Systems Audit and Control Association, Rolling Meadows, IL.

Bayuk, J. (2009). Enterprise security for the executive.

Bayuk, J. L. (2007). Stepping Through the InfoSec Program. ISACA.

Bayuk, J. L. (2024). Stepping through cybersecurity risk management: a systems thinking approach. John Wiley and Sons.

Bayuk, J., and Price Waterhouse, L. L. P. (1997). Security through process management. Price Waterhouse.

Beasley, M. S., Branson, B. C., Braumann, E. C., and Pagach, D. P. (2023). Understanding the ecosystem of enterprise risk governance. The Accounting Review, 98(5), 99–128.

Beasley, M. S., Clune, R., and Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. Journal of Accounting and Public Policy, 24(6), 521–531.

Beasley, M., Pagach, D., and Warr, R. (2008). Information conveyed in hiring announcements of senior executives overseeing enterprise-wide risk management processes. Journal of Accounting, Auditing and Finance, 23(3), 311–332.

Bell, T., Peecher, M. E., and Solomon, I. (2002). The strategic-systems approach to auditing. Cases in Strategic-Systems Auditing, 1–34.

Bensaada, I., and Taghezout, N. (2019). An enterprise risk management system for SMEs: innovative design paradigm and risk representation model. Small Enterprise Research, 26(2), 179–206.

Bharadwaz, D. J., and Goswami, K. C. (2023). Enterprise Risk Management Practices in India: A Case Study of Select Indian Companies.

Bharathy, G. K., and McShane, M. K. (2014). Applying a Systems Model to Enterprise Risk Management. Engineering Management Journal, 26(4).

Boardman, J., and Sauser, B. (2008). Systems thinking: Coping with 21st century problems. CRC Press.

Brockett, P. L., Golden, L. L., and Wolman, W. (2012). Enterprise cyber risk management. Risk Management for the Future–Theory and Cases, 319–340.

Bromiley, P., McShane, M., Nair, A., and Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. Long Range Planning, 48(4), 265–276.

Cboe Global Markets. (2024, August). Risk committee charter. https://s202.q4cdn.com/174824971/files/doc_governance/2024/Aug/cboe-global-markets-risk-committee-charter.pdf

Chmielecki, T., Cholda, P., Pacyna, P., Potrawka, P., Rapacz, N., Stankiewicz, R., and Wydrych, P. (2014). Enterprise-oriented cybersecurity management. 2014 Federated Conference on Computer Science and Information Systems, 863–870.

Cholez, H., and Feltus, C. (2014). Towards an innovative systemic approach of risk management. Proceedings of the 7th International Conference on Security of Information and Networks, 61–64.

Chunying, Z., and Weiqing, G. (2009). Risk management based on data warehouse of securities companies. 2009 4th International Conference on Computer Science and Education, 819–822.

CoinDesk. (2025, May 19). Binance, Kraken thwarted social engineering attacks similar to Coinbase hack. https://www.coindesk.com/web3/2025/05/19/binance-kraken-thwarted-social-engineering-attacks-similar-to-coinbase-hack

Collins, M. (2024). Systems Thinking in Cybersecurity; Ending with the Beginning in Mind. Journal of Systems Thinking Preprints.

Creswell, J. W., and Poth, C. N. (2016). Qualitative inquiry and research design: Choosing among five approaches. Sage publications.

CrowdStrike. (2024, August 6). Channel File 291 incident: Root cause analysis. https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf

Deane, J. K., Goldberg, D. M., Rakes, T. R., and Rees, L. P. (2019). The effect of information security certification announcements on the market value of the firm. Information Technology and Management, 20, 107–121.

Dombalagian, O. H. (2020). Securities and Derivatives Exchanges in the United States: Market and Ownership Structures. Financial Market Infrastructure: Law and Regulation (OUP, Forthcoming 2021), Tulane Public Law Research Paper, 20–14.

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. Journal of Cybersecurity, 5(1), tyz013.

Fox Business. (2025, May). Coinbase estimates cyberattack could cost crypto exchange up to $400 million. https://www.foxbusiness.com/markets/coinbase-estimates-cyberattack-could-cost-crypto-exchange-up-to-400-million

Garrett, G. A. (2018). Cybersecurity in the Digital Age: Tools, Techniques, and Best Practices. Aspen Publishers.

Ghon Rhee, S. (2000). Risk management systems in clearing and settlement: Asian and Pacific equity markets. Asian Development Review, 18(01), 94–119.

Gjerdrum, D., and Peter, M. (2011). The new international standard on the practice of risk management–A comparison of ISO 31000: 2009 and the COSO ERM framework. Risk Management, 31(21), 8–12.

Gordon, L. A., Loeb, M. P., and Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? Journal of Computer Security, 19(1), 33–56.

Gordon, L. A., Loeb, M. P., Zhou, L., and Wilford, A. L. (2024). Empirical evidence on disclosing cyber breaches in an 8-K report: Initial exploratory evidence. Journal of Accounting and Public Policy, 46, 107226.

Gottipati, H. (2020). A proposed cybersecurity model for cryptocurrency exchanges.

Greenberg, A. (2019). Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Anchor.

Grünbichler, A., and Errath, W. (2007). Enterprise Risk Management: A View from the Insurance Industry. LAW AND ECONOMICS OF RISK IN FINANCE, Peter Nobel and Marina Gets, Eds, 111–120.

Haywood, L. K., Forsyth, G. G., De Lange, W. J., and Trotter, D. H. (2017). Contextualising risk within enterprise risk management through the application of systems thinking. Environment Systems and Decisions, 37, 230–240.

Hoyt, R. E., and Liebenberg, A. P. (2011). The value of enterprise risk management. Journal of Risk and Insurance, 78(4), 795–822.

Innerhofer-Oberperfler, F., and Breu, R. (2006). Using an Enterprise Architecture for IT Risk Management. ISSA, 1–12.

Intercontinental Exchange, Inc. (2023, March). Risk Committee Charter. https://s2.q4cdn.com/154085107/files/doc_downloads/2023/Intercontinental-Exchange-Inc.-Risk-Committee-Charter-March-2023-Clean.pdf

Jimmy, F. N. U. (2024). Assessing the Effects of Cyber Attacks on Financial Markets. Journal of Artificial Intelligence General Science (JAIGS) ISSN: 3006-4023, 6(1), 288–305.

Johnson, K. N. (2015). Cyber risks: Emerging risk management concerns for financial institutions. Ga. L. Rev., 50, 131.

Kammoun, N., Bounfour, A., Özaygen, A., and Dieye, R. (2019). Financial market reaction to cyberattacks. Cogent Economics and Finance, 7(1), 1645584.

Karaca, S. S., Şenol, Z., and Korkmaz, Ö. (2018). Mutual interaction between corporate governance and enterprise risk management: A case study in Borsa Istanbul Stock Exchange. Muhasebe ve Finansman Dergisi, 78.

Karanja, E. (2017). Does the hiring of chief risk officers align with the COSO/ISO enterprise risk management frameworks? International Journal of Accounting and Information Management, 25(3), 274–295.

Kountur, R. (2018). The likelihood value of residual risk estimation in the management of enterprise risk. Investment Management and Financial Innovations, 15(3), 49–55.

Krueger, T. (2006). Stock Settlement and Clearance in the United States. Journal of Finance Issues, 4(1), 171–179.

Kurniawanti, I. A. (2010). Critiques Towards Coso's Enterprise Risk Management (ERM) Framework in Its Basic Assumptions. Majalah Ekonomi Universitas Airlangga, 20(3), 4119.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659–671.

Lee, L. S., and Green, E. (2015). Systems thinking and its implications in enterprise risk management. Journal of Information Systems, 29(2), 195–210.

Leyla Acaroglu. (2017, September 17). Tools for Systems Thinkers: The 6 Fundamental Concepts of Systems Thinking. Https://Medium.Com/Disruptive-Design/Tools-for-Systems-Thinkers-the-6-Fundamental-Concepts-of-Systems-Thinking-379cdac3dc6a.

Liedtka, J. (2018). Why design thinking works. Harvard Business Review, 96(5), 72–79.

Lundqvist, S. A. (2014). An exploratory study of enterprise risk management: Pillars of ERM. Journal of Accounting, Auditing and Finance, 29(3), 393–429.

Malhotra, Y. (2015). Cybersecurity and Cyber-Finance Risk Management: Strategies, Tactics, Operations, and, Intelligence: Enterprise Risk Management to Model Risk Management: Understanding Vulnerabilities, Threats, and Risk Mitigation (Presentation Slides). Tactics, Operations, and, Intelligence: Enterprise Risk Management to Model Risk Management: Understanding Vulnerabilities, Threats, and Risk Mitigation (Presentation Slides)(September 15, 2015).

Malik, M. F., Zaman, M., and Buckby, S. (2020). Enterprise risk management and firm performance: Role of the risk committee. Journal of Contemporary Accounting and Economics, 16(1), 100178.

Marchetti, A. M. (2011). Enterprise risk management best practices: From assessment to ongoing compliance (Vol. 561). John Wiley and Sons.

Mathrani, S., and Mathrani, A. (2013). Utilizing enterprise systems for managing enterprise risks. Computers in Industry, 64(4), 476–483.

McLucas, A. C. (2003). Decision making: risk management, systems thinking and situation awareness. Argos Press P/L.

Milne, A. (2007). The industrial organization of post-trade clearing and settlement. Journal of Banking and Finance, 31(10), 2945–2961.

Moşteanu, N. R. (2020). Challenges for organizational structure and design as a result of digitalization and cybersecurity. The Business and Management Review, 11(1), 278–286.

Munusamy, T., Khodadadi, T., and Zamani, M. (2023). Enhancing Cyber Security in Organisations by Establishing Attributes Towards Achieving Cyber Resilience.

M'manga, A. (2020). Designing for cyber security risk-based decision making. Bournemouth University.

Nasdaq, Inc. (2025, February 19). Audit and Risk Committee Charter. https://ir.nasdaq.com/static-files/8889423a-e0b7-4408-9cd9-4094b2a43fc6

National Institute of Standards and Technology. (2020). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). NIST Cybersecurity Framework.

National Institute of Standards and Technology. (2021). NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide.

National Institute of Standards and Technology. (2022). NIST IR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM).

Naudet, Y., Mayer, N., and Feltus, C. (2016). Towards a systemic approach for information security risk management. 2016 11th International Conference on Availability, Reliability and Security (ARES), 177–186.

Oosthoek, K., and Doerr, C. (2020). Cyber security threats to Bitcoin exchanges: Adversary exploitation and laundering techniques. IEEE Transactions on Network and Service Management, 18(2), 1616–1628.

O'Donnell, E. (2005). Enterprise risk management: A systems-thinking framework for the event identification phase. International Journal of Accounting Information Systems, 6(3), 177–195.

Perera, A. A. S. (2019). Enterprise risk management–international standards and frameworks. International Journal of Scientific and Research Publications, 9(7), 211–217.

Perlroth, N. (2021). This is how they tell me the world ends: The cyberweapons arms race. Bloomsbury Publishing.

Rabinowitz, R. (2020). From Securities to Cybersecurity: The SEC Zeroes in on Cybersecurity. BCL Rev., 61, 1535.

Romanosky, S., and Petrun Sayers, E. (2021). Enterprise risk management: Understanding the role of cyber risk. TPRC49: The 49th Research Conference on Communication, Information and Internet Policy.

Russo, D., Hart, T. L., and Schönenberger, A. (2002). The evolution of clearing and central counterparty services for exchange-traded derivatives in the United States and Europe: a comparison. ECB Occasional Paper, 5.

Saleem, K. S. A., Zraqat, O. M., and Okour, S. M. (2019). The effect of internal audit quality (IAQ) on enterprise risk management (ERM) in accordance to COSO framework. European Journal of Scientific Research, 152(2), 177–188.

Salim, H. M. (2014). Cyber safety: A systems thinking and systems theory approach to managing cyber security risks (Doctoral dissertation, Massachusetts Institute of Technology).

Sax, J., and Andersen, T. J. (2019). Making risk management strategic: Integrating enterprise risk management with strategic planning. European Management Review, 16(3), 719–740.

Schneier, R., and Miccolis, J. (1998). RISK: Enterprise management. Strategy and Leadership, 26(2), 10–16.

Seiersen, R. (2022). The Metrics Manifesto: Confronting Security with Data. John Wiley and Sons.

Shaked, A., Tabansky, L., and Reich, Y. (2020). Incorporating systems thinking into a cyber resilience maturity model. IEEE Engineering Management Review, 49(2), 110–115.

Sharma, U., Chapman, T., and Garrison, S. W. (2021). Addressing Risks Across the Organization: Enterprise Risk Management. Journal: American Water Works Association, 113(5).

Siegel, C. A., Sagalow, T. R., and Serritella, P. (2002). Cyber-risk management: technical and insurance controls for enterprise-level security. In Information Security Management Handbook, Volume 4 (pp. 357–380). Auerbach Publications.

Sion, L., Yskout, K., Van Landuyt, D., and Joosen, W. (2018). Risk-based design security analysis. Proceedings of the 1st International Workshop on Security Awareness from Design to Deployment, 11–18.

Smith, K. T., Jones, A., Johnson, L., and Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society, 17(1), 42–60.

Spafford, E. H., Metcalf, L., and Dykstra, J. (2023). Cybersecurity myths and misconceptions: Avoiding the hazards and pitfalls that derail us. Addison-Wesley Professional.

Stave, K., and Hopper, M. (2007). What constitutes systems thinking? A proposed taxonomy. 25th International Conference of the System Dynamics Society, 29.

Sterman, J. D. (2000). Systems thinking and modeling for a complex world. Management, 6(1), 7-17.

Stine, K., Quinn, S., Witte, G., and Gardner, R. K. (2020). Integrating cybersecurity and enterprise risk management (ERM). National Institute of Standards and Technology, 10.

Stoll, M. (2015). From information security management to enterprise risk management. Innovations and Advances in Computing, Informatics, Systems Sciences, Networking and Engineering, 9–16.

Supervision, B. (2011). Basel committee on banking supervision. Principles for Sound Liquidity Risk Management and Supervision (September 2008).

Tahir, I. M., and Razali, A. R. (2011). The relationship between enterprise risk management (ERM) and firm value: Evidence from Malaysian public listed companies. International Journal of Economics and Management Sciences, 1(2), 32–41.

Taran, Y., Boer, H., and Lindgren, P. (2013). Incorporating enterprise risk management in the business model innovation process. Journal of Business Models, 1(1).

Trautman, L. J., and Newman, N. (2022). A Proposed SEC Cyber Data Disclosure Advisory Commission. Securities Regulation Law Journal, 50(3), 199.

U.S. Securities and Exchange Commission. (2014). Regulation Systems Compliance and Integrity (Reg SCI). Final Rule, Release No. 34-73639; File No. S7-01-13.

U.S. Securities and Exchange Commission. (2023). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. Final Rule, Release No. 33-11216.

U.S. Securities and Exchange Commission. (2023). Form 10-K: Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934.

U.S. Securities and Exchange Commission. (2023). Form 8-K, Item 1.05: Material Cybersecurity Incidents.

Varma, J. R. (2009). Risk Management Lessons from the Global Financial Crisis for Derivative Exchanges.

White, D. (1995). Application of systems thinking to Risk Management: A review of the literature. Management Decision, 33(10), 35–45.

Williamson, D. (2007). The COSO ERM framework: a critique from systems theory of management control. International Journal of Risk Assessment and Management, 7(8), 1089–1119.

Yin, R. K. (2017). Case study research and applications: Design and methods. Sage publications.

APPENDIX A

INTERVIEW APPROACH AND TOPICS

Section	**Topic**
1	Introduction and Consent
2	Cybersecurity Risk Perception

Section	Topic
3	Governance Structures and Board Oversight
4	Regulatory Disclosures and Materiality
5	Lessons Learned
6	Closing and Recommendations

Section 1: Introduction and Consent

This interview explores how your organization governs cybersecurity risk and aligns it with enterprise risk management, particularly in light of recent regulatory changes and high-profile cyber incidents. Your insights will remain confidential and anonymized in any outputs. May I have your permission to proceed?

Section 2: Cybersecurity Risk Perception

Objective: Understand how the organization frames cyber risk.

Questions:

1. How does your organization currently define and categorize cybersecurity risk within the ERM framework?
2. In your view, has the perception of cybersecurity risk changed at the executive or board level over the last 3 years?
3. Is cyber risk viewed more as a technical issue or a strategic business risk? Why?

Section 3: Governance Structures and Board Oversight

Objective: Examine organizational governance mechanisms.

Questions:

4. Does your institution have a dedicated cyber risk committee or is it integrated into broader risk/audit committees?

5. Who typically participates in cross-functional cyber risk governance meetings? How often do they meet?

6. What kind of decisions are made in these meetings (e.g., risk appetite, incident review, budget approval)?

7. Are cyber metrics (e.g., patch compliance, SIEM alerts, CSFs) incorporated into board reporting or dashboards?

8. Have cyber tabletop exercises or simulations been conducted at the board or executive level?

Section 4: Regulatory Disclosures and Materiality

Objective: Understand approaches to compliance and external reporting.

Questions:

9. How has the SEC's 2023 cybersecurity disclosure rule (Form 10-K and 8-K Item 1.05) impacted your governance practices?

10. What processes exist to assess the materiality of a cyber incident?

11. Who is involved in making the disclosure decision within the 4-business-day window?

12. Do you maintain formal playbooks or escalation matrices for such disclosures?

13. How do you coordinate between Legal, IR, Risk, and InfoSec during incidents?

Section 6: Closing and Recommendations

Objective: Capture future outlook and expert opinion.

Questions:

14. What governance model do you believe works best for aligning cyber risk with ERM?

15. If you could recommend one change to improve cyber risk governance across the industry, what would it be?

16. Is there anything else you'd like to share that might help inform this research?