Institute of Banking Studies Research >>

Consultancy and Research Department

Governance of Cybersecurity in Banking and Financial Organizations.

Facts and trends of how cybersecurity is governed within organizational structures in the banking/financial sectors (GCC and global perspectives)

This research was conducted by

Dr.Haidar Almohri External Consultant

in collaboration with Cybersecurity R&D Lab (CYS-LAB), the Central Bank of Kuwait.

December 2024

Table of Contents

Glossary ***I***

1. Introduction ***1***

1.1 Drivers of Cybersecurity Governance in Banking and Financial Institutions 2

2. Methodology ***4***

3. Shifting Paradigms in Cybersecurity Governance for Banking and Finance ***6***

3.1 Impact of Major Cyber Events on Governance Practices 6

4. Cybersecurity governance and organizational structure ***7***

4.1 Centralization of Cybersecurity Governance and the Evolving Role of the CISO 7

4.2 Enhancing Cybersecurity Governance through RACI Matrix and Three Lines of Defense 7

4.3 Strategic Integration of CISOs in Banking and Financial Institutions' Cybersecurity Governance 8

5. The Influence of Government Policies and Global Frameworks on Cybersecurity Governance in Banking and Financial Institutions ***8***

5.1 USA 9

5.2 Europe 12

5.3 China 15

5.4 GCC 17

5.5 International Organizations 20

6. Results and discussion ***20***

6.1 Organizational Profile 20

6.2 Organizational Cybersecurity Context **23**

6.3 Leadership, Commitment and Cybersecurity Culture 25

6.4 Planning and risk management 28

6.5 Support and Resources 31

6.6 Operations and incident management 32

6.7 Performance evaluation and continual improvement 36

6.8 Compliance and legal requirement 37

6.9 Concluding Thoughts 39

7. Summary and Conclusion ***40***

7.1 Limitations and future work 43

References ***44***

Glossary

1. **Bank for International Settlements (BIS)**: An international financial organization that supports central banks in their pursuit of monetary and financial stability. BIS provides frameworks and guidelines, including those related to operational resilience and cybersecurity governance, for global banking and financial institutions.
2. **European Central Bank (ECB)**: The central bank responsible for monetary policy within the Eurozone. The ECB oversees banking and financial institutions in the region and ensures their resilience, including through its Cyber Resilience Oversight Expectations (CROE), which addresses cybersecurity risks.
3. **Financial Stability Board (FSB)**: An international body that coordinates the development of policies to promote financial stability worldwide. The FSB plays a key role in shaping cybersecurity practices for banking and financial institutions, ensuring global cooperation and effective risk management.
4. **Federal Banking and Financial Institutions Examination Council (FFIEC)**: A U.S. government interagency body responsible for establishing principles and standards for the examination of banking and financial institutions. The FFIEC provides tools like the Cybersecurity Assessment Tool to help institutions evaluate their cybersecurity preparedness.
5. **Cybersecurity Governance**: The processes, policies, and responsibilities through which an organization manages its cybersecurity strategy and risks. Effective cybersecurity governance ensures alignment with business goals and regulatory requirements, fostering accountability across all levels of the organization.
6. **Three-Lines-of-Defense Model**: A widely adopted governance framework that divides risk management responsibilities into three layers:

    - **First Line:** Operational units managing day-to-day risks.
    - **Second Line:** Risk management and compliance overseeing risk controls.
    - **Third Line:** Internal audit providing independent assurance on risk management practices.

7. **Chief Information Security Officer (CISO)**: The senior executive responsible for overseeing an organization's cybersecurity program. The CISO develops and enforces policies to protect the organization's information assets from cyber threats and ensures compliance with regulatory requirements.
8. **ISO 27001**: An international standard for managing information security. It provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) to protect sensitive information.
9. **NIST Cybersecurity Framework (CSF)**: A voluntary framework created by the U.S. National Institute of Standards and Technology (NIST) that provides a structured approach for managing and reducing cybersecurity risks. The framework is built around five core functions: Identify, Protect, Detect, Respond, and Recover.
10. **CIS Controls**: A set of best practices for cybersecurity, developed by the Center for Internet Security (CIS). These controls provide organizations with actionable steps to improve their security posture and defend against common cyberattacks.
11. **Cybersecurity Maturity**: A measure of an organization's progress and capability in managing cybersecurity risks. Maturity levels range from basic, ad-hoc cybersecurity practices to more advanced, proactive, and well-integrated cybersecurity strategies.
12. **Cyber Incident Response**: The process through which an organization manages and responds to cybersecurity events, such as data breaches or attacks. This includes identifying the incident, containing the threat, eradicating the issue, and recovering from its effects.
13. **Cybersecurity Organizational Structure**: The way an organization assigns and manages cybersecurity responsibilities. This can include centralized structures, where a dedicated cybersecurity team handles security, or decentralized structures where cybersecurity duties are spread across departments.
14. **Cybersecurity Framework**: A set of guidelines and standards designed to help organizations manage cybersecurity risks. Examples include ISO 27001, NIST CSF, and the CIS Controls, which provide structured approaches for improving cybersecurity posture.

15. **RACI MATRIX**: A responsibility assignment matrix. RACI is an acronym derived from the four key responsibilities most typically used: Responsible, Accountable, Consulted, and Informed. It is used for clarifying and defining roles and responsibilities in cross-functional or departmental projects and processes.

1. Introduction

The safe and efficient operation of financial organizations is essential for maintaining and promoting financial stability and economic growth. If not properly managed, such organizations can become sources of financial shocks, such as liquidity dislocations and credit losses, or major channels through which these shocks are transmitted across domestic and international financial markets.

However, rapid technological advancements have exposed banking and financial institutions to a growing landscape of cyber threats. Robust cybersecurity governance is now critical for protecting sensitive data, preventing financial fraud, and maintaining the trust of customers and other stakeholders.

Cybersecurity governance refers to the formal structures, policies, and processes that a financial organization establishes to manage and mitigate cyber risks. It encompasses the entire lifecycle of cybersecurity governance, from establishing strategic objectives to implementing controls and monitoring their effectiveness.

Effective cybersecurity governance hinges on the implementation of a comprehensive cybersecurity framework. A cybersecurity framework provides a structured set of guidelines, standards, and best practices that an organization follows to manage cybersecurity risks. It forms the foundation for creating secure and resilient digital environments by setting clear processes for identifying, mitigating, responding to, and recovering from cyber threats. Essentially, a cybersecurity framework serves as a blueprint for building, maintaining, and continuously improving an organization's security posture.

A robust cybersecurity framework not only safeguards the organization’s operations but also supports its financial stability goals. It defines how the organization will protect its information systems, prevent unauthorized access, and respond to security incidents, all while maintaining operational efficiency. The framework outlines specific security controls, processes, and policies that the organization must implement.

In the context of financial and banking institutions, adopting a cybersecurity framework ensures the protection of critical assets, such as customer data and financial information,

while also complying with regulatory requirements. For instance, the Central Bank of Kuwait (CBK) mandates that Kuwaiti banks adopt recognized frameworks like ISO 27001, which focuses on establishing, implementing, maintaining, and continually improving an information security management system (ISMS). By doing so, organizations not only enhance their security posture but also build trust with customers, regulators, and stakeholders by demonstrating their commitment to protecting sensitive information and mitigating cybersecurity risks.

Effective cybersecurity governance is crucial for establishing a systematic and proactive approach to managing the ever-evolving cyber threats faced by banking and financial institutions. It not only fosters the appropriate consideration and management of cyber risks at all organizational levels but also ensures the allocation of adequate resources and expertise to effectively address them [1].

1.1 Drivers of Cybersecurity Governance in Banking and Financial Institutions

Cybersecurity governance in banking and financial institutions is influenced by multiple drivers, each contributing to the development of robust security frameworks. These drivers ensure institutions can effectively mitigate cyber risks and maintain stability within the financial system. The key drivers include regulatory requirements, market and competition pressures, general governance practices, and technological advancements.

1. **Regulatory Requirements**: Banking and financial institutions face stringent regulatory mandates globally that enforce cybersecurity governance. Regulatory authorities such as the European Central Bank (ECB), the Prudential Regulation Authority (PRA) in the United Kingdom, and the Office of the Comptroller of the Currency (OCC) in the United States establish and enforce standards for operational resilience, including measures to address cyber risks.
    - For instance, the Basel Committee on Banking Supervision (BCBS) guidelines emphasize operational resilience and cybersecurity as critical components of banking oversight, requiring institutions to adopt cybersecurity governance frameworks [13].

- Similarly, the General Data Protection Regulation (GDPR) in Europe mandates that banking and financial institutions adopt strict data security measures, with significant penalties for non-compliance [16].
- National regulatory bodies such as the Office of the Comptroller of the Currency (OCC) in the United States also implement and oversee cybersecurity assessment frameworks to safeguard the resilience of the banking systems they regulate.

Thus, compliance with regulatory requirements is one of the primary drivers that compel banking and financial institutions to establish comprehensive cybersecurity governance practices.

2. **Market and Competitive Pressures**: The banking and financial sector operates in a highly competitive environment, where reputation and trust are pivotal. In recent years, customer preferences have shifted toward institutions that demonstrate strong cybersecurity measures, particularly as digital banking platforms become more prevalent.
    - J.P. Morgan Chase reportedly invests over $600 million annually in cybersecurity, viewing it as essential not just for risk mitigation but also for maintaining customer trust and competitive advantage [17]. This demonstrates how market competition is driving institutions to prioritize cybersecurity governance.
    - A report by Deloitte highlights that cybersecurity has become a key differentiator for banking and financial institutions, with customers more likely to choose banks that invest in security as a core part of their digital strategy [18].

The growing awareness of cybersecurity risks among customers, coupled with the increasing adoption of digital platforms, forces banking and financial institutions to adopt robust cybersecurity governance to remain competitive in the market.

3. **General Governance Practices and Risk Management**: Cybersecurity governance is increasingly seen as part of broader good governance and risk management practice. Banking and financial institutions are integrating cybersecurity into their corporate governance frameworks to address operational risks and protect their assets.

- A study by PwC showed that 79% of banking executives consider cybersecurity to be a board-level priority, reflecting its growing importance in corporate governance [19].
- The implementation of frameworks like ISO 27001 and the NIST Cybersecurity Framework has become standard practice, where institutions integrate cybersecurity governance into their overall risk management strategies to ensure operational continuity and reduce financial losses due to cyber incidents.

Cybersecurity is no longer isolated as an IT function but is embedded into the core governance structures of banking and financial institutions, driven by the need to protect critical assets and maintain operational resilience.

4. **Technological Innovation and Digital Transformation**: The increasing reliance on digital banking services, mobile applications, and fintech solutions has expanded the attack surface for cyber threats. This digital transformation necessitates enhanced cybersecurity governance to protect institutions from sophisticated cyberattacks.
    - As banking and financial institutions increasingly adopt cloud computing, artificial intelligence, and blockchain technologies, they face new cybersecurity challenges. A report by McKinsey & Company notes that digital innovation is one of the biggest drivers pushing banking and financial institutions to strengthen their cybersecurity governance to manage these new risks [20].
    - The rapid growth of FinTech has also increased regulatory scrutiny, with new market players required to follow the same stringent cybersecurity governance practices as established banking and financial institutions [21].

The evolving digital landscape is a major driver, forcing institutions to continuously adapt their cybersecurity governance to keep pace with technological advancements.

2. Methodology

To assess cybersecurity governance practices within banking and financial institutions, a questionnaire was distributed to a broad selection of organizations. While many organizations

were targeted, a total of 46 responses were received. This sample encompassed a diverse range of financial entities, including banks, investment management firms, monetary authorities, and other financial service providers. The survey aimed to evaluate the current state of cybersecurity governance by gathering data on various aspects critical to a robust security posture. The collected data has been extensively analyzed to understand how the participating banking and financial institutions implement cybersecurity governance frameworks within their organizations [9].

A comprehensive questionnaire was developed to assess key aspects of cybersecurity governance within participating banking and financial institutions. This instrument aimed to capture the methods employed for cybersecurity governance and the overall maturity level of cybersecurity practices. The questionnaire comprised 41 questions categorized into ten core topics. The initial section (six questions) focused on gathering organizational profile information. Subsequent sections addressed critical areas such as:

- Organizational cybersecurity context
- Leadership commitment and cybersecurity culture
- Planning and risk management strategies
- Support and resource allocation
- Operations and incident management procedures
- Performance measurement and continuous improvement processes
- Compliance with relevant legal and regulatory requirements

The selection of these core topics aligns with the essential parameters for effective cybersecurity governance as outlined in international standards, guidelines, and frameworks. A copy of the survey is provided in Appendix A. Additionally, to facilitate visualization of the collected data, a dashboard has been developed. This interactive tool allows users to explore the findings in greater detail. [For access to the dashboard, please see the link: https://report.maticandemo.com (clickable in electronic version of the article)].

3. Shifting Paradigms in Cybersecurity Governance for Banking and Finance

In recent years, cybersecurity governance in banking and financial institutions has undergone a significant shift, moving from a purely technical concern within IT departments to an integral part of enterprise risk management. Research from Gartner indicates that most banking and financial institutions are adopting a centralized governance model where the Chief Information Security Officer (CISO) reports directly to the Chief Risk Officer (CRO) or Board of Directors, rather than to the Chief Information Officer (CIO) [10,11,12]. This separation from IT ensures that cybersecurity is treated as a governance issue, enhancing the independence and objectivity of the security function, which is crucial for meeting regulatory and compliance requirements.

3.1 Impact of Major Cyber Events on Governance Practices

This shift has been significantly influenced by key events exposing systemic vulnerabilities and highlighting the need for robust cybersecurity governance. The **2008 financial crisis** revealed deficiencies in risk management and corporate governance [24], demonstrating that technical solutions alone were insufficient without strong oversight [25]. This led to increased board-level engagement in cybersecurity and the integration of cyber risk into enterprise risk management.

The **2016 Bangladesh Bank robbery**, involving the theft of $81 million via the SWIFT network [26], was a failure of both technical defenses and governance practices like inadequate controls and non-compliance with protocols [27]. This event prompted a global reassessment of cybersecurity governance, emphasizing the need to combine technical measures with strong governance mechanisms.

Events like the WannaCry ransomware attack and the Equifax data breach in 2017 caused widespread disruptions and significant financial losses [28][29], affecting reputation and stakeholder trust. Consequently, organizations began adopting more rigorous governance practices, such as appointing cybersecurity experts to boards [30].

Collectively, these events led to a paradigm shift in perceiving cybersecurity. There was growing recognition that cyber risks are strategic threats requiring direct oversight from executive leadership [31]. Regulatory frameworks like the General Data Protection Regulation (GDPR)

mandated stringent data protection measures and held organizations accountable at the governance level [32]. Organizations started integrating cybersecurity into overall risk management and fostering a culture where security is everyone's responsibility [33].

4. Cybersecurity governance and organizational structure

4.1 Centralization of Cybersecurity Governance and the Evolving Role of the CISO

A survey conducted by Gartner with 130 asset-intensive organizations revealed that 74% of respondents had centralized their cybersecurity governance under a central cybersecurity team or an enterprise steering committee. This shift towards centralization helps ensure consistency in policy application, risk management, and operational oversight across departments. More importantly, this move elevates the CISO's role from that of a tactical control owner to a strategic facilitator, positioning cybersecurity governance as a key part of enterprise risk management [22].

4.2 Enhancing Cybersecurity Governance through RACI Matrix and Three Lines of Defense

Some studies highlight the importance of utilizing a RACI matrix to define roles across legal, compliance, audit, and risk functions, ensuring clear accountability and collaboration. Legal teams ensure compliance with cyber regulations, compliance officers oversee regulatory adherence, and internal audit provides independent assurance of the effectiveness of cybersecurity controls [23].

The Three-Lines-of-Defense model is crucial in this context, with internal audit in the third line providing oversight and assurance, risk management in the second line assessing the organization's risk profile, and operational management (first line) responsible for implementing cybersecurity controls. This model reinforces a multistakeholder approach to cybersecurity governance, where each department contributes to a comprehensive risk management strategy [23].

4.3 Strategic Integration of CISOs in Banking and Financial Institutions' Cybersecurity Governance

This trend is also observed in banking and financial institutions, where the CISO's involvement in enterprise governance is increasingly seen as essential for aligning cybersecurity with broader business objectives. As financial organizations digitize and face more sophisticated cyber threats, the need for cross-functional steering committees that include senior management, IT, risk, and compliance teams has become evident. These committees ensure that cybersecurity governance is embedded at the strategic level, with direct reporting lines to senior leadership and the board.

5. The Influence of Government Policies and Global Frameworks on Cybersecurity Governance in Banking and Financial Institutions

Current research on cybersecurity in banking and financial institutions primarily emphasizes global government policies and frameworks. Establishing common goals, implementation strategies, and clear stakeholder roles are seen as crucial for comprehensive cybersecurity. Indeed, government policies and regulations have significantly influenced banking and financial institutions' adoption of robust cybersecurity frameworks. Consequently, examining governmental structures, along with established public-private guidelines and standards, is essential to gaining a deeper understanding of cybersecurity governance practices within financial organizations.

Effective national cybersecurity necessitates a collaborative framework. This framework should facilitate cooperation between public and private stakeholders in developing cybersecurity policy and implementing operational measures. Ideally, governments, businesses, civil society, and individual users would work together to create a multi-layered defense incorporating technical safeguards (e.g., standards), procedural controls (e.g., guidelines, best practices), and personnel training. Examples include promoting the adoption of international cybersecurity framework and standards (like ISO 27001 and NIST) and implementing certification schemes (like Public Key Infrastructure) by both government and industry [2].

To understand the global landscape of cybersecurity governance in banking and finance, this section explores policies, regulations, and guidelines established by governments, public sector entities, and private industry leaders in the world's major economies.

5.1 USA

In the United States, banking and financial institutions are organized and regulated based on the services the institutions provide. The profile of the banking and financial sector is best described by defining the services offered, which includes: (1) deposit, consumer credit, and payment systems products; (2) credit and liquidity products; (3) investment products; and (4) risk transfer products.

Banking and financial institutions within the sector continuously assess their cybersecurity posture to mitigate cyber incident risks. This ongoing process involves understanding vulnerabilities, staying informed about the evolving threat landscape, and adapting security and resilience strategies accordingly. Risk assessments are a long-standing and accepted practice within the Financial Services Sector and are widely conducted by individual institutions and expected by regulators.

To assess overall sector risk, the U.S. Department of the Treasury, financial regulators, Homeland Security, law enforcement, and other government partners collaborate with banking and financial institutions. This collaboration involves information sharing on current and emerging threats, developing mitigation strategies, and identifying critical assets requiring special attention. Collaboration occurs through regular meetings, incident data exchange, co-created threat information, and regulatory processes.

Banking and financial institutions and technology service providers operate in a tightly interconnected ecosystem. Incidents impacting one firm can quickly cascade and disrupt others, even across sectors. This vulnerability is amplified by the fact that banking and financial institutions primarily rely on external services like electricity, communications, and transportation.

To comprehensively manage cyber risk, many institutions work to identify their most sensitive infrastructure and processes and implement stronger safeguards. Equally important is identifying critical institutions within the banking and financial sector. This ensures a swift recovery of their essential operations in the event of a disruption, regardless of the cause. Identifying these key components is also essential for developing and continuously refining business continuity plans and recovery protocols, ensuring the financial system's resilience in the face of cyberattacks or other disruptions.

Owners and operators of identified critical infrastructure whose business and operations depend on an extensive network of information and communications technology and software (or “cyber dependent”) may be eligible for access to classified government cybersecurity threat information as appropriate. Cyber-dependent critical infrastructure may also be prioritized for routine and incident-driven cyber technical assistance activities offered by the US Department of Homeland Security (DHS) and other agencies.

In response to cybersecurity and physical threats, the banking and financial sector fosters collaboration across a vast network. This network encompasses industry participants (companies and trade associations), federal and state government agencies, including financial regulators, as well as international partners. Their collective efforts, spanning local, national, and global levels, aim to strengthen the sector's overall security and resilience.

The Financial Services Sector’s umbrella organizations for critical infrastructure protection are the private-sector-led Financial Services Sector Coordinating Council (FSSCC) and the government-led Financial and Banking Information Infrastructure Committee (FBIIC). The FSSCC and FBIIC respectively serve as the Sector Coordinating Council and Government Coordinating Council for the Financial Services Sector.

The Financial Services Sector critical infrastructure partnership includes a variety of stakeholders in addition to the FSSCC and FBIIC:

- Private Sector: FSSCC, Financial Services Information Sharing and Analysis Center (FSISAC), individual firms, trade associations, regional coalitions, security service providers, technology service providers, and industry partners from other sectors;

- Executive Branch: Treasury, DHS (including the United States Secret Service), U.S. Department of Justice (including the Federal Bureau of Investigation), U.S. Department of Defense, and other departments and agencies;
- Financial Regulators: FBIIC agencies, which includes banking and credit union regulators; securities regulators; self-regulatory organizations; and State regulators;
- State, Local, Tribal, and Territorial Partners; and
- International: Non-U.S. based banking and financial institutions and service providers, non-U.S. regulators, and non-U.S. law enforcement, intelligence communities, and homeland security government partners.

The FSSCC and its member organizations promote sector security and resilience through information sharing, incident response and recovery efforts, and by advocating for best practices and effective policies. Additionally, the FS-ISAC, the operational arm of the FSSCC, disseminates specific cybersecurity and physical risk information along with recommendations for protective measures and practices to thousands of institutions across the sector.

Highly regulated by authorities that oversee and examine banking and financial institutions, the Financial Services Sector relies on the FBIIC, a government coordinating council, to facilitate collaboration among financial regulators and the Treasury Department. This collaboration focuses on critical infrastructure resilience, including information sharing, best practices, and incident response. The sector's cybersecurity posture has been further strengthened by close collaboration with the National Institute of Standards and Technology (NIST) on developing the NIST Cybersecurity Framework.

Financial Services Sector companies were closely involved in the development of the NIST Cybersecurity Framework, and they continue to make progress in implementing it. This work has been aided not only by a close partnership with NIST, but also through the work of FSSCC, FBIIC, FS-ISAC, and sector trade associations.

In addition, the Federal Financial Institution Examination Council (FFIEC) issued a cybersecurity self-assessment tool in 2015 to help institutions identify their risks and determine their cybersecurity preparedness. [3]

5.2 Europe

The European Union boasts a robust cybersecurity landscape for the banking and financial sector. Several key organizations play a vital role, including the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), the European Insurance and Occupational Pensions Authority (EIOPA), the European Union Agency for Cybersecurity (ENISA), and the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) [38].

The European Commission (EC), a key executive body of the European Union, plays a pivotal role in shaping the EU's overall cybersecurity strategy and banking and financial sector policies. In 2018, the EC issued the Fintech Action Plan [4] with the primary objective of bolstering cyber resilience within the banking and financial sector. This plan is achieved by:

- Facilitating information sharing on cyber threats among market participants.
- Promoting greater supervisory convergence and enforcement of IT risk management.
- Enhancing EU coordination in cyber threat testing through a common threat-intelligence-led approach.

In September 2020, the EU adopted a digital finance strategy outlining how Europe can navigate the digital transformation of finance in the coming years, while mitigating associated risks. The strategy focuses on four key areas:

- Removing fragmentation in the Digital Single Market
- Adapting the EU regulatory framework to facilitate digital innovation
- Promoting data-driven finance [5]
- Addressing challenges and risks associated with digital transformation, including enhancing the digital operational resilience of the financial system [6].

The European Commission (EC) has proposed a regulation requiring all financial entities, including credit institutions, payment and e-money institutions, insurance companies, and others, to ensure they can withstand all types of ICT (Information and Communication Technology) disruptions and threats. These entities will need to comply with strict standards to prevent and minimize the impact of ICT-related incidents.

Furthermore, the EC's proposal establishes an oversight framework for service providers (e.g. Big Tech companies), that deliver critical ICT services to financial entities.

The European Banking Authority (EBA) is an independent EU authority focused on the banking and financial sector. Its primary function is to contribute to the European Single Rulebook, which aims to establish a harmonized set of prudential rules for all EU banking and financial institutions.

In the realm of ICT/cybersecurity, the EBA has issued several regulatory documents, including guidelines, recommendations, opinions, and other non-regulatory public statements.

In November 2019, the EBA issued a pivotal set of guidelines (EBA/GL/2019/04) on ICT and security risk management. These guidelines emphasize the importance of robust internal governance and a well-defined internal control framework. This framework ensures clear responsibility allocation across all staff levels, including management bodies, for effectively managing and mitigating ICT and security risks faced by banking and financial institutions.

The EU Delegated Regulation on strong customer authentication, built upon the European Banking Authority's (EBA) Regulatory Technical Standards for secure communication and strong customer authentication (SCA), targets credit institutions, payment institutions, and electronic money institutions. This regulation outlines a range of security measures, including secure communication standards for third-party providers interacting with account servicing payment service providers within the EU/EEA during the provision of payment initiation or account information services. It's noteworthy that the EBA developed the regulation in close cooperation with the European Central Bank (ECB).

The EBA, in collaboration with the ECB, has established guidelines on incident reporting under the Revised Payment Services Directive (PSD2, EU directive 2015/2366). These guidelines define the criteria, thresholds, and methodology for credit institutions, payment institutions, and electronic money institutions within the EU/EEA to determine whether an operational or security incident related to payment services qualifies as major, and thus requires notification to the competent authority in their home member state.

The EBA Guidelines on reporting retail payment fraud under PSD2 directly support the directive's objective of enhancing security for EU retail payments. These guidelines require credit institutions, payment institutions, and electronic money institutions to collect and report data on both payment transactions and fraudulent transactions.

The ECB has published cyber resilience oversight expectations for financial market infrastructures. The ECB's Cyber Resilience Oversight Expectations (CROE) is a key framework for financial market infrastructures in Europe, promoting stringent cyber resilience measures [14]. Based on these expectations, the financial market infrastructure should use leading international, national and industry-level standards, guidelines or recommendations (e.g. NIST, COBIT 5 and ISO/IEC 27000, etc.), reflecting current industry best practices in managing cyber threats, as a benchmark for designing its cyber resilience framework and incorporating the most effective cyber resilient solutions [1].

The Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) serves as a platform for strategic dialogue among financial market infrastructures. Its core objectives are to:

- Raise awareness of the topic of cyber resilience
- Catalyse joint initiatives to develop effective solutions for the market.
- Provide a place to share best practices and foster trust and collaboration.

The ECRB is comprised of representatives of pan-European financial market infrastructures and their critical service providers.

Established in 2008, the European Financial Institutes – Information Sharing and Analysis Centre (FI-ISAC) fosters secure and effective information sharing among banking and financial institutions. This independent organization brings together a diverse membership, including country representatives from the banking and financial sector, national CERTs (GovCerts), and Law Enforcement Agencies (LEAs).

This information exchange system benefits all members, including banks within their member states. It facilitates awareness-raising on potential cyber risks and provides early warnings about emerging threats. The FI-ISAC's mission focuses on information exchange across various

channels: electronic and mobile channels, credit/debit cards, central systems, and all ICT-related topics. This includes:

- Cybercriminal activity targeting the financial community
- Vulnerabilities, technology trends, and evolving threats
- Incident reports and case studies

Members share information via meetings, forwarding continuously relevant information to the EU FI-ISAC list server, and through direct communication between member organizations/individuals.

5.3 China

A report about “cybersecurity and the impact on banks in China, regulatory policy development and update” was published in 2015 and is available online [7]. This part of the article mainly presents the important points of that report.

China's cybersecurity policies encompass various stakeholders within the banking industry: the government, regulatory bodies (like the China Banking Regulatory Commission - CBRC), banking and financial institutions, and IT companies.

Under the enforcement of the CBRC, banking and financial institutions need to review and amend IT strategy and planning, management systems, governance structures, people management, innovation mechanisms, performance evaluations, system development, and technology procurement to drive effective compliance with the regulations. Banks in China should pay particular attention to the following areas:

- **Governance system:** Establish a steering committee and response team comprised of key business functions and departments. This team will be responsible for leading the implementation plan and overseeing its execution across the entire bank.
- **Infrastructure development:** Prioritize the implementation of "secure and controllable IT" in peripheral technologies like network, storage, and security devices, followed by core technologies like mainframe computers. Banks should aim for a year-on-year increase in the use of secure and controllable solutions within peripheral systems.

Additionally, increased investment in research and development of domestic expertise for "secure and controllable IT" is crucial.

- **Supporting Frameworks:** The regulations will directly impact banks' existing management frameworks, particularly those related to risk management and information security. This necessitates adjustments to risk tolerance levels, the risk assessment framework, and risk monitoring indicators. Additionally, banks will need to enhance their information security standards to align with the new requirements.

In addition to the previously mentioned points, the following paragraphs draw upon a report [8] to provide a concise overview of China's cyber laws and regulations concerning financial organizations and their impact on the operations of international banking and financial institutions.

To ensure data security compliance, Chinese banking and financial institutions leverage government-issued data classification standards like JR/T 0197-2020 (Financial Data Security—Guidelines for Data Security Classification). These standards guide institutions in classifying data based on its potential impact on national security, public interests, and business operations. Additionally, Chinese law mandates businesses to maintain agile data inventories that allow for ongoing data reclassification.

Local banking and financial institutions, including multinational banks, must understand the key data localization regulators and the specific industry requirements for data storage and cross-border data transfer management in China. Cross-border data transfers are subject to approval by the Cyberspace Administration of China (CAC) based on a demonstrated business need. To obtain approval, banks must undergo a CAC security assessment, acquire data subject consent, and conduct a thorough internal risk assessment. Additionally, the data classification of the information being transferred may also influence the approval process.

To ensure swift and uniform responses to data breaches, data controllers must establish effective and enforceable incident response plans. In the event of a data breach, entities must comply with government-defined notification requirements. These include notifying regulators and effected parties within 72 hours. For breaches involving personal or important data of over 100,000

individuals, a stricter timeframe applies. In such cases, controllers must inform the Cyberspace Administration of China (CAC) within eight hours of the breach. Following the resolution of an incident, a subsequent report must be submitted to the CAC within five business days.

5.4 GCC

The GCC region, encompassing Kuwait, Saudi Arabia, the UAE, Bahrain, Oman, and Qatar, has seen rapid digital transformation, especially in its banking and financial sector. With the rise in cyber threats, GCC countries have introduced robust cybersecurity governance frameworks to protect critical infrastructure. Central banks play a vital role in enforcing cybersecurity regulations, ensuring compliance to safeguard the financial system.

5.4.1 Central Bank of Kuwait (CBK) Cybersecurity Framework (CSF)

The Central Bank of Kuwait (CBK) has established a comprehensive Cybersecurity Framework (CSF) in January 2020, designed to enhance the resilience of the banking sector against evolving cyber threats. As per the Central Bank of Kuwait (CBK) regulations, all Kuwaiti banks are required to adopt cybersecurity frameworks aligned with ISO 27001 standards, part of the broader ISO 27000 series. This ensures that banks implement best practices in information security management, ensuring a high level of protection against cyber threats. Kuwaiti banks use this framework to align their Cybersecurity Resilience Program with international standards, facilitating continuous improvements in risk management and compliance [34].

A core principle of the CBK's Cybersecurity Framework is cybersecurity governance, emphasizing that accountability begins with the board of directors (BoD). According to the regulations, the BoD holds ultimate responsibility for cybersecurity governance within their organizations. This accountability includes overseeing cyber risk governance, approving cybersecurity policies, and ensuring their effective implementation. To achieve this, the framework mandates that both the BoD and senior management must possess adequate cybersecurity expertise and engage in continuous learning to stay updated on emerging trends and threats.

The framework further outlines that regulated entities should establish robust cybersecurity governance structures that cascade from the board level down through audit functions, risk

functions, security operations, and IT operations. This governance flow ensures that accountability is maintained in the organization, creating a security-oriented culture.

By enforcing such standards, CBK ensures that banks can handle evolving cyber risks while maintaining business continuity, safeguarding customer information, and protecting the banking sector from major disruptions.

In accordance with the CBK guidelines, all regulated entities are required to establish cybersecurity governance frameworks within their organizations. Responsibility begins with the Board of Directors (BoD) and extends through the Audit function, risk management function, security operations, and IT operations. Effective governance of cybersecurity risk, both at an individual organizational level and sectoral level, ensures the security, safety, and resilience of the Kuwait Banking Sector.

Aligned with Kuwait's National Cybersecurity Strategy, the CBK Cybersecurity Framework (CSF) establishes a comprehensive framework to assess and enhance the cybersecurity maturity and response capabilities of Regulated Entities (REs) within the banking sector. This framework focuses on improving cyber crisis management through standardized practices across the sector. CBK requires REs to complete self-assessments using its Cybersecurity Readiness Assessment Template, enabling banks to evaluate their preparedness and inherent risks regularly [34].

The CSF emphasizes:

- **Crisis Management**: Ensuring that all REs have the capability to manage and recover from cyber crises efficiently.
- **Maturity Improvement**: Mandating continuous assessment and updating of cybersecurity practices, using templates designed to track maturity improvements over time.
- **Sector-Wide Coordination**: In the event of significant incidents, the CBK leads a sector-wide response, fostering collaboration across banks to mitigate risks [34].

5.4.2 Broader GCC Cybersecurity Practices

In addition to Kuwait, other GCC nations have adopted similar regulatory frameworks:

- **Saudi Arabia**: The Saudi Central Bank (SAMA) enforces a Cybersecurity Framework that emphasizes risk management, incident response, and security awareness programs across banking and financial institutions [35].
- **United Arab Emirates**: The Central Bank of the UAE introduced regulations requiring banking and financial institutions to strengthen their cybersecurity posture through threat detection, response mechanisms, and compliance with international standards [36].
- **Qatar**: The Qatar Central Bank (QCB) has developed a cybersecurity strategy focusing on mitigating advanced persistent threats (APTs) and ensuring sector-wide resilience [37].
- **Oman**: The Central Bank of Oman (CBO) has issued the Regulatory Framework of Cyber Security and Resilience to set minimum requirements across licensed institutions. The CBO aims to set requirements in licensed institutions to address and strengthen their management of cyber security risks. It also aims to reach the same level of maturity of cyber security controls across the licensed institutions [39].
- **Bahrain**: The Central Bank of Bahrain (CBB) mandates a robust cybersecurity framework to ensure that banking and financial institutions manage and mitigate cyber risks effectively. The CBB's regulations require licensees to report cybersecurity incidents within one hour of detection to the CBB using their prescribed reporting formats. Additionally, banking and financial institutions are required to establish a cybersecurity risk management framework that includes incident detection, risk mitigation, and recovery plans. The framework is intended to foster resilience against cyber threats, enhance the security of information assets, and ensure compliance with international standards such as ISO27001 [40].

5.4.3 Role of Regulators in Enforcing Cybersecurity Governance

Central banks across the GCC enforce cybersecurity governance through regulatory inspections, mandatory reporting, and compliance with national frameworks. These central banks regularly conduct cyber crisis exercises, requiring Regulated Entities to perform ongoing assessments and ensure that cybersecurity practices evolve in response to emerging threats. This collaborative and adaptive approach enhances the resilience of the banking and financial sector across the region [34][35][36][37].

5.5 International Organizations

In addition to national and regional entities, international organizations such as the Bank for International Settlements (BIS) and the Financial Stability Board (FSB) have played a significant role in shaping cybersecurity governance frameworks for the banking sector. The BIS, through its Basel Committee on Banking Supervision, provides global guidance on operational and cybersecurity resilience, urging banks to enhance their risk management practices [13]. Furthermore, the FSB has developed a Cyber Lexicon and issued guidelines to harmonize global cybersecurity standards, focusing on building resilience against cyber threats across the international financial system [15]. The World Bank supports countries in assessing cybersecurity maturity, establishing cybersecurity governance structures, and strengthening institutions for implementation. This includes developing legal and regulatory frameworks for cybercrime and cybersecurity along with national-level cybersecurity strategies [41]. These organizations collectively drive the global agenda for improving cybersecurity governance within the banking and financial sector, ensuring a unified approach to managing cyber risks.

6. Results and discussion

6.1 Organizational Profile

This section of the questionnaire gathered basic organizational information to facilitate further analysis of the survey data. Questions focused on the following:

- Name of the organization
- Location

- Specific field of activity (industry)
- Size of the organization

A total of 46 banking and financial institutions responded to the questionnaire. The breakdown by industry is as follows:

- 29 Banks
- 8 Financial Services Firms
- 7 Monetary Authority (Central Banks)
- 1 Fintech Company
- 1 Investment Management Organization

Geographically, the respondents were distributed as follows:

- 30 from GCC Countries
- 5 from Europe
- 5 from East Asia
- 6 from USA, Canada, Argentina, Mexico, Morocco, and New Zealand (one participant from each country)

This section assessed the participants' perceptions of their organizations' cybersecurity maturity level. Figure 1 presents a visual representation of the distribution of responses for this key question.

The survey results revealed variations in perceived cybersecurity maturity levels across participating institutions. Seventeen respondents, comprising:

- Thirteen institutions from the GCC region
- Two institutions from Europe
- One institution from East Asia
- One institution from Canada

indicated an advanced level of cybersecurity maturity. Notably, eleven out of these seventeen institutions have more than 2,000 employees.

Conversely, nine institutions reported being at a developing stage of cybersecurity maturity. This group included:

- Six institutions from the GCC region
- One institution from Europe
- Two institutions from East Asia

An additional eleven GCC organizations, two European organizations, two East Asian organizations, and one organization from the United States, one from New Zealand, one from Morocco, one from Argentina and one from Mexico identified themselves as being at the established level of maturity (Figure 2).

Figure 1 shows that more than 63 percent of the respondents think they are not at the advance level of the cybersecurity maturity. They feel a gap between what they are and what they should be.

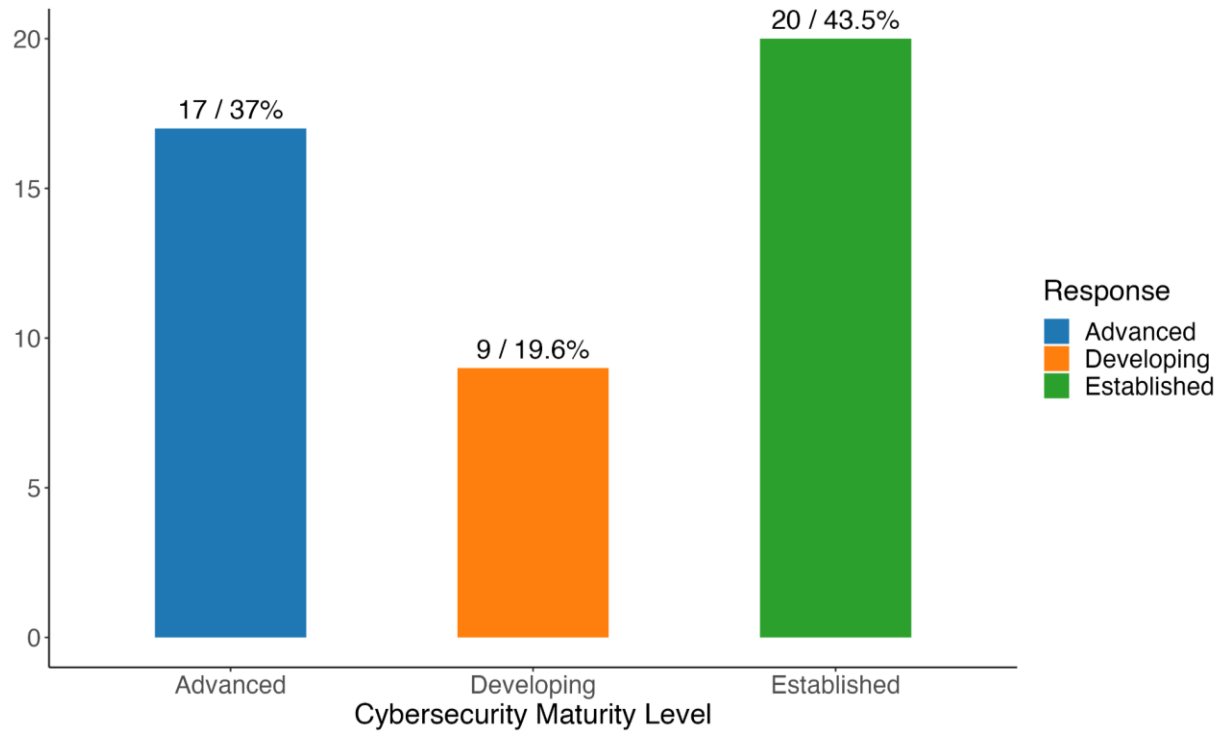

Figure 1. cyber security maturity in the participants organization

6.2 Organizational Cybersecurity Context

This section of the questionnaire explored the cybersecurity management frameworks employed by participating institutions. It investigated the specific frameworks each organization utilized, the duration of their implementation, the established organizational structure for cybersecurity governance, and the identification of key stakeholders involved in cybersecurity efforts. This comprehensive approach aimed to assess the selection and depth of implementation of cybersecurity management systems within the participating banking and financial institutions.

A key question within this section focused on the specific cybersecurity frameworks implemented by each participating institution. Based on their responses, we categorized the organizations into five distinct groups.

Category 1: This group comprises the institutions implementing the most comprehensive set of the common cybersecurity control frameworks, encompassing **ISO 27000, NIST Cybersecurity Framework (CSF), and CIS Controls**.

Category 2: Institutions in this category have adopted **ISO 27000 along with either NIST CSF or CIS Controls**.

Category 3: Institutions in this category rely **solely on ISO 27000** for their cybersecurity framework.

Category 4: This group of institutions **have not** implemented the **ISO 27000 but they utilize the NIST framework with or without CIS control**.

Category 5: This final category encompasses institutions that have adopted **alternative** cybersecurity frameworks, **excluding ISO 27000, NIST and CIS control.** Examples of such frameworks include PCI DSS (Payment Card Industry Data Security Standard), or other industry-specific frameworks. Table 1 summarizes the developed categories.

Category	Framework Adoption
1	ISO 27000 + NIST Cybersecurity Framework (CSF) + CIS Controls

2	ISO 27000 + NIST CSF / CIS Controls.
3	ISO 27000
4	NIST / NIST + CIS
5	Other Frameworks

Table 1: Categories based on the adopted on the cybersecurity framework adopted

Figure 2 illustrates the geographic distribution of participating institutions across the five identified framework adoption categories.

To gain deeper insights, responses from the survey will be subjected to a comparative analysis. The analysis will compare and contrast responses across the predefined categories established earlier (Figure 2). This approach aims to identify any variations or consistencies in cybersecurity governance practices among different types of institutions.

Analysis of survey data revealed a strong emphasis on dedicated cybersecurity structures within banking and financial institutions. Notably, across all categories except the second, virtually every institution has a department or dedicated team specifically responsible for cybersecurity within their organizational chart. This finding underscores the growing recognition of cybersecurity as a critical priority in the banking and financial sector.

As illustrated in Figure 3, survey responses regarding the method of cybersecurity responsibility distribution within banking and financial institutions reveal a clear preference for centralized structures. The figure highlights that a significant majority of institutions across all categories (except Category 2) favor a centralized approach with a dedicated cybersecurity team. Notably, in Category 1, nearly all institutions (93%) have adopted this model.

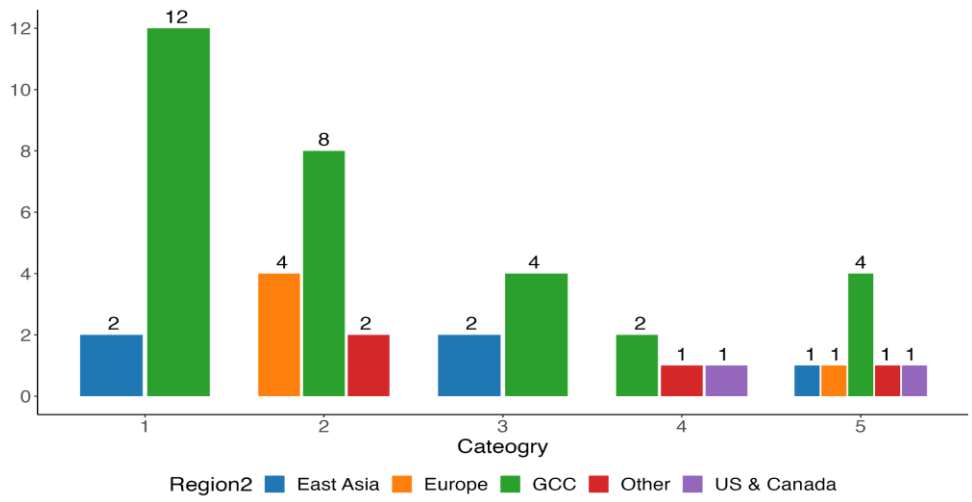

Figure 2. Number of participant Institutions in different categories with their geographical group

Survey responses regarding the identification of primary internal and external cybersecurity stakeholders, and the level of fulfillment of their requirements, are presented in Figure 4. Notably, all institutions in Category 1 demonstrate a strong commitment to cybersecurity governance by identifying their primary internal and external stakeholders and fully meeting their requirements. However, a gap emerges in Categories 2 through 5. While most institutions in these categories have identified their stakeholders, there seems to be a disparity in fully fulfilling their requirements. Further investigation is necessary to understand the reasons behind this gap. Additionally, a small number of organizations in Category 1 (7%) and Category 4 (25%) did not respond to this question, potentially affecting the overall percentages for these categories.

6.3 Leadership, Commitment and Cybersecurity Culture

This section explores leadership, organizational commitment, and cybersecurity culture within banking and financial institutions. Survey responses shed light on how management teams demonstrate leadership and commitment to effective cybersecurity management.

Encouragingly, a survey question regarding the alignment between institutions' strategic direction and cybersecurity policies and objectives revealed a strong focus on integration. Forty-three institutions responded, and all but two (both located in the GCC) indicated that their cybersecurity efforts are aligned with their overall strategic direction. This finding underscores

the growing recognition of cybersecurity as a critical component of achieving strategic goals within the banking and financial sector.

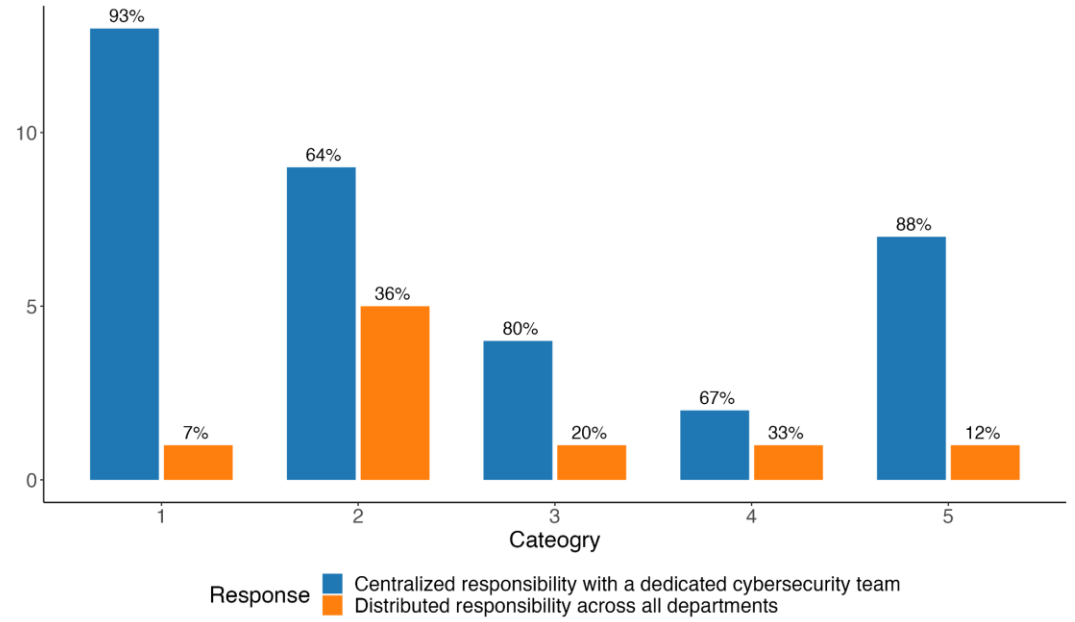

Figure 3. cybersecurity responsibility model distribution across different department

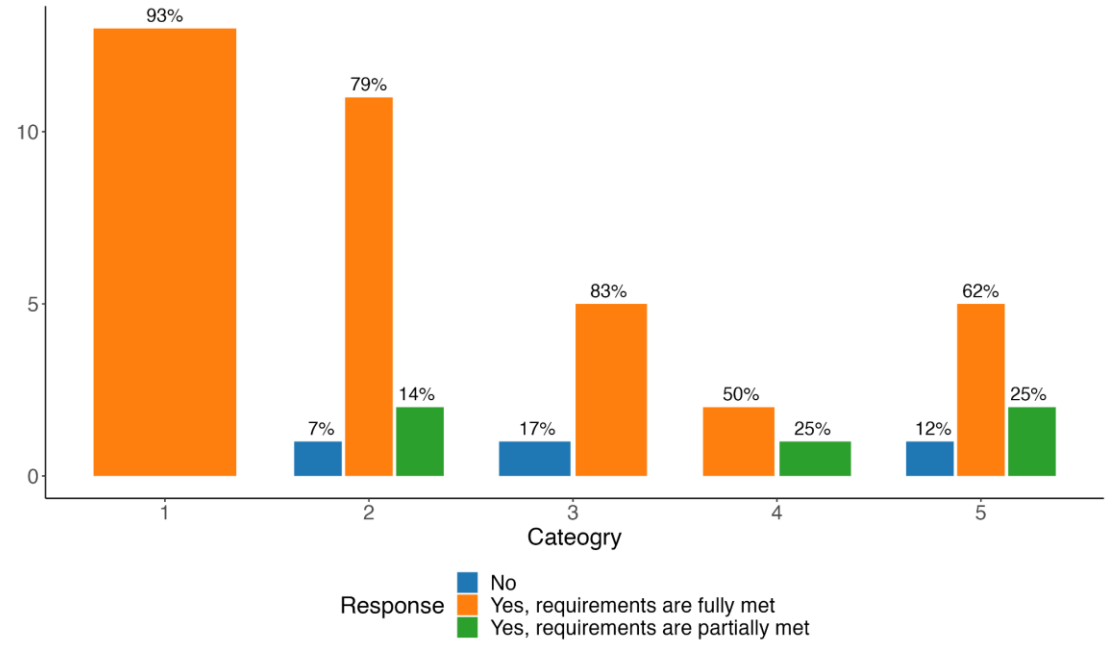

Figure 4. Identification of cybersecurity stakeholders and fulfilment of their requirements

The survey findings and analysis of organizational practices highlight the growing trend toward centralized cybersecurity governance in banking and financial institutions. Centralizing governance under the CISO, with direct reporting to the CRO or Board of Directors, ensures that cybersecurity is treated as a core business risk. This structure is becoming the norm in banking and financial institutions, allowing for clearer accountability and reducing the conflicts of interest that can arise when the CISO reports to the CIO [10,12].

Further, centralization of cybersecurity governance helps create consistency in policies and strategies across the organization, particularly in large banking and financial institutions. However, some organizations employ decentralized models, often involving Business Information Security Officers (BISOs) who manage local cybersecurity activities, while the central cybersecurity governance team retains overall strategic control [10]. This hybrid model allows for a balance between global oversight and localized adaptability.

To gauge the level of commitment from top management towards cybersecurity governance, a survey question was specifically designed to gauge top management commitment to cybersecurity governance. This assessment focused on three key indicators:

- **Endorsement of Cybersecurity Policies:** This option assessed whether top management actively endorses and promotes established cybersecurity policies within the organization.
- **Allocation of Dedicated Resources:** This indicator focused on whether top management allocates sufficient resources, such as personnel and budget, specifically for cybersecurity initiatives.
- **Direct Involvement in Initiatives:** This option evaluated the extent to which top management directly participates in cybersecurity initiatives, demonstrating their active engagement in the process.

Figure 5 reveals insights into how management teams within banking and financial institutions demonstrate their commitment to cybersecurity. The survey allowed participants to select

multiple options, so the cumulative percentage across responses may exceed 100%. Here's a breakdown of the key findings:

Endorsement of Cybersecurity Policies: A significant majority of institutions (represented by the highest bar in Figure 5) prioritize endorsement of cybersecurity policies as a primary approach. This highlights the importance of clear and well-defined policies in establishing a strong cybersecurity foundation.

Allocation of Dedicated Resources: Resource allocation for cybersecurity is another crucial commitment area, as shown in Figure 5. While endorsement receives the highest response, dedication of resources is still a significant focus for many institutions.

Direct Involvement in Initiatives: Direct involvement in cybersecurity initiatives by top management, though receiving the fewest endorsements compared to the other two options in Figure 5, still demonstrates a commitment to active leadership in cybersecurity efforts.

In addition, the finding that nearly 90% of participants reported buy-in for the cybersecurity strategy from all business units further reinforces a strong cybersecurity culture within these institutions. An organizational culture that prioritizes cybersecurity across all departments is essential for effective implementation of security measures.

6.4 Planning and risk management

This section focuses on risk assessment methods, plans, and procedures employed by banking and financial institutions to manage cybersecurity threats. The survey covered six questions to gather insights into these critical aspects of cybersecurity governance.

Figure 6 illustrates the various processes followed by organizations to identify and prioritize cybersecurity risks. Here's a breakdown of the most common approaches, as indicated by the graph:

- **Conducting Regular Risk Assessment Exercises:** This appears to be the most prevalent method, with a high percentage of respondents likely endorsing this practice.

- **Using Risk Management Frameworks:** The graph indicates that a significant portion of organizations leverage established frameworks (e.g., ITAR, NIST, and AMF) to guide their risk management activities.
- **Involving Cross-Functional Teams:** Collaboration across different departments is another key strategy, as reflected in the graph. This ensures a comprehensive perspective when identifying and prioritizing cybersecurity risks.

The survey revealed a strong emphasis on documenting cybersecurity risk experience and treatment methods. Notably, all but two responding institutions reported maintaining a dedicated document or database for this purpose. This highlights the importance of learning from past experiences and establishing a knowledge base for effective risk management.

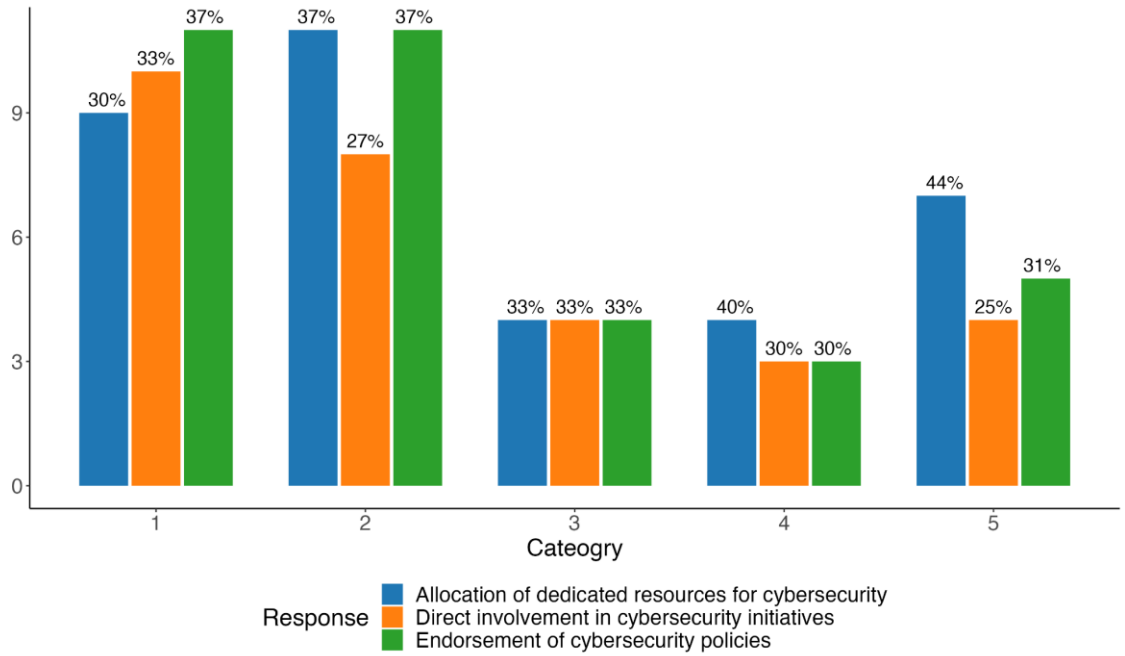

Figure 5. Distribution of responses to the question about the management commitments

Furthermore, nearly 90% of participants indicated that their risk strategies consider all the most important factors. This suggests a commitment to thorough risk assessments that encompass a broad range of potential threats and vulnerabilities.

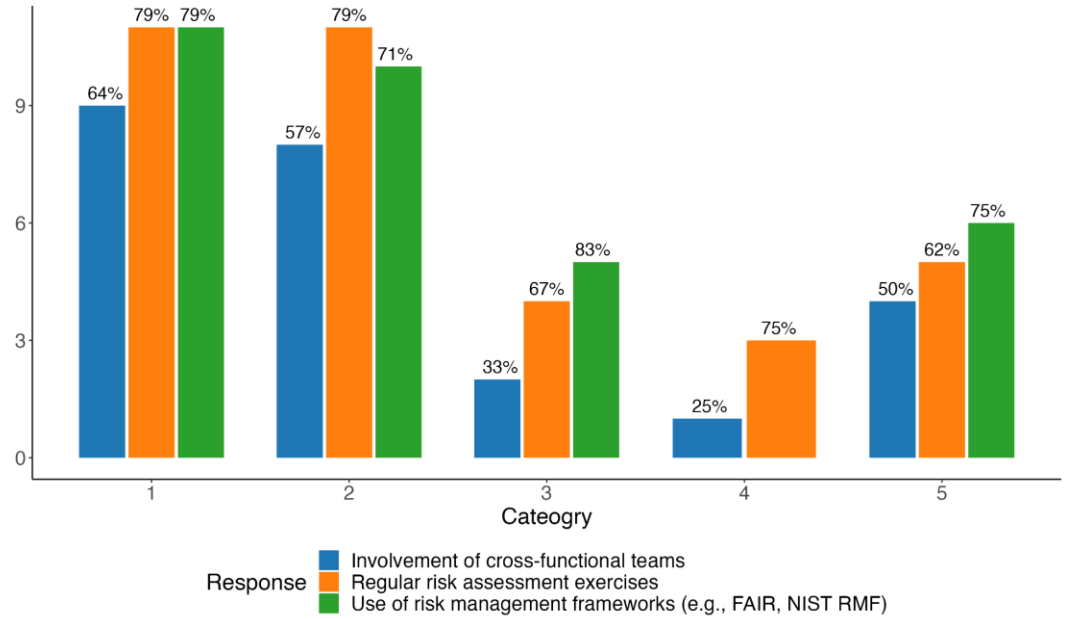

Figure 6. Risk assessment process followed by organizations

Figure 7 sheds light on the risk appetite distribution across different categories of banking and financial institutions participating in the survey. The graph suggests a general preference for low-risk appetite across most categories.

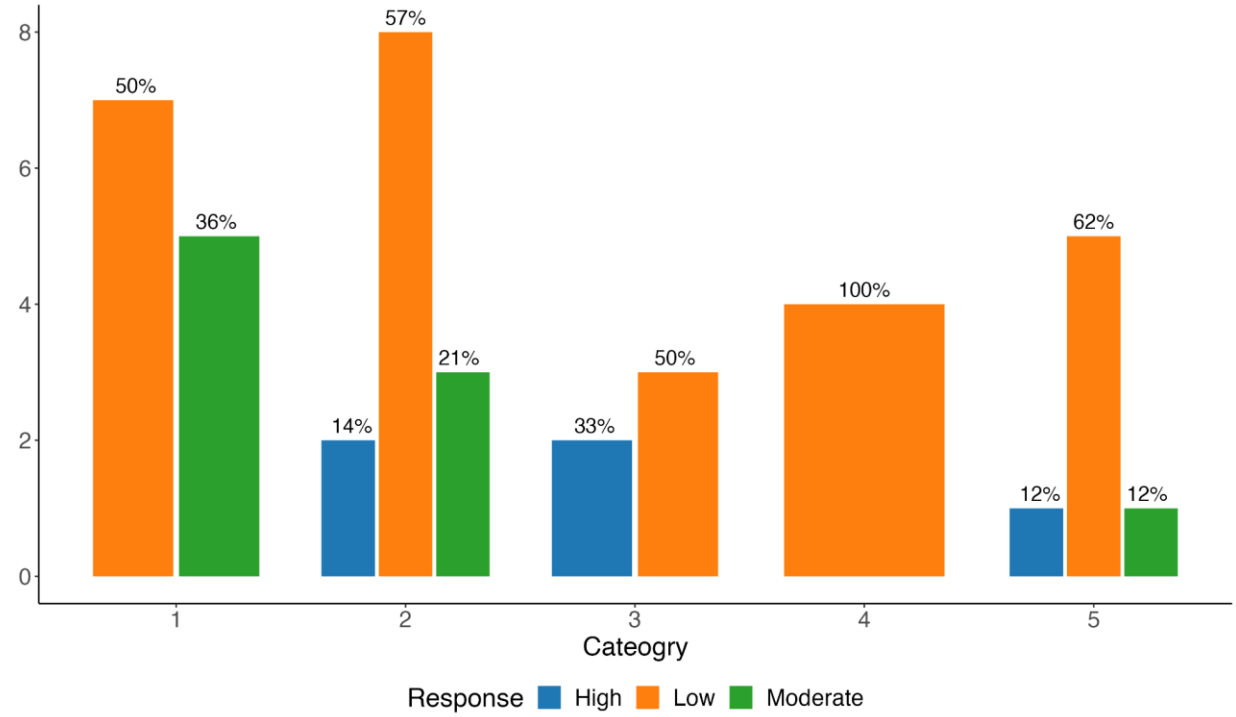

Figure 7. Organization's risk appetite

6.5 Support and Resources

This section explores resource allocation for cybersecurity governance through two survey questions: one focusing on the percentage of IT budgets dedicated to cybersecurity, and another on participants' perception of resource adequacy for cybersecurity efforts.

Figure 8 reveals a clear distinction in cybersecurity resource allocation across the various framework categories established earlier. The graph illustrates the percentage of IT budget dedicated to cybersecurity within each category. We can see that in category 1, a significant majority of institutions in allocate more than 15% of their IT budget to cybersecurity. This suggests a substantial investment in cybersecurity resources within this category compared to others. on the other hand, Institutions in Categories 3, 4, and 5 dedicate a smaller portion of their IT budget (less than 15%) to cybersecurity, as shown by the shorter bars in Figure 8. This may indicate a lower risk profile for these categories, or a potential need for resource optimization in their cybersecurity efforts.

The next survey question explored participants' perceptions of resource adequacy for implementing and maintaining cybersecurity measures. The results are illustrated in Figure 9. Technological tools received the highest endorsement across all categories, as indicated by the tallest bar in Figure 9. This suggests that most institutions, regardless of category, view themselves as adequately equipped with the necessary technological tools for cybersecurity.

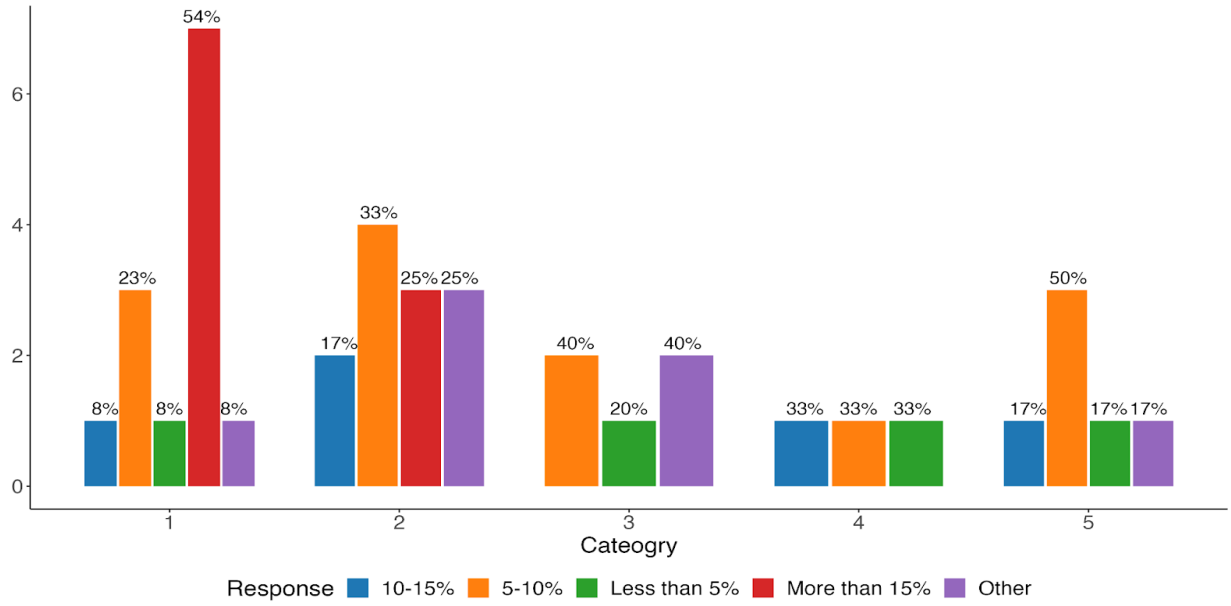

Figure 8. Percentage of the IT budget dedicated in cybersecurity per category

6.6 Operations and incident management

This section focuses on the strategies employed by banking and financial institutions for managing cybersecurity incidents and preventing future occurrences. The survey covered questions in two key areas:

- **Cybersecurity Incident Management:** This section explores the methods used by institutions to identify, respond to, and recover from cybersecurity incidents.
- **Prevention and Mitigation Techniques:** This section examines the tools, processes, and instructions utilized by institutions to proactively prevent cyber incidents and mitigate potential damage.

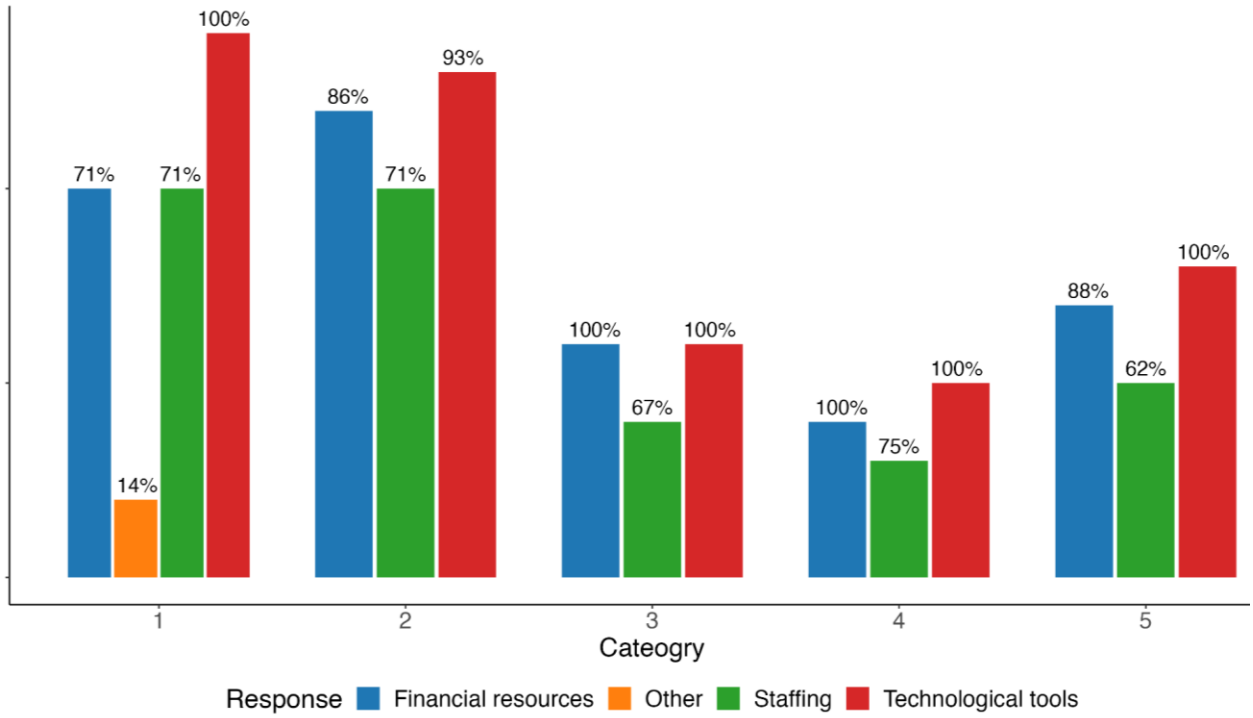

Figure 9. Adequacy and availability of resources in each category

Survey responses regarding the methods used by institutions for controlling and managing operational processes related to cybersecurity are presented in Figure 10.

Here's a breakdown of the most prevalent approaches, as indicated by the graph:

- **Regular Reviews and Audits:** This appears to be the most widely used method, with a high percentage of respondents likely endorsing this practice. Regular reviews and audits help to identify and address weaknesses in operational processes before they can be exploited.
- **Policy and Procedure Implementation:** The graph indicates that a significant portion of organizations rely on implementing well-defined policies and procedures to guide their cybersecurity operations. This ensures a consistent and standardized approach to security controls.
- **Use of Automation Tools:** While not as prevalent as the previous two methods, the use of automation tools is also reflected in the graph, suggesting that some institutions

leverage technology to streamline and improve the efficiency of their cybersecurity operations.

We notice that Institutions in Category 1 exhibit the most comprehensive approach, with a high bar for all of the methods in Figure 10. This suggests they leverage a combination of regular reviews and audits, policy and procedure implementation, and automation tools for robust operational control. Institutions in Categories 2 and 4 also demonstrate a strong emphasis on operational control, as indicated by the significant bars for all of the options in Figure 10. Institutions in Categories 3 and 5 appear to rely more heavily on regular security audits and assessments (as indicated by the prominent bars for these options in Categories 3 and 5 of Figure 10). While they may utilize some additional methods, the overall approach seems less comprehensive compared to Category 1.

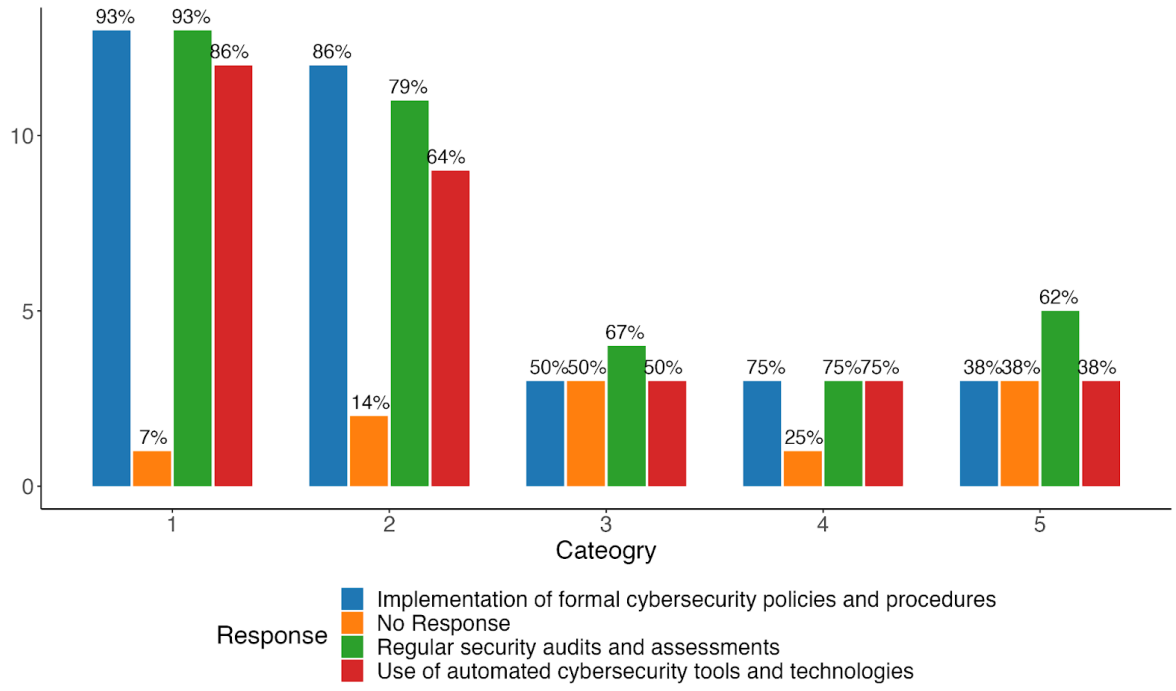

Figure 10. Methods used in different categories for controlling and managing operational processes related to cybersecurity

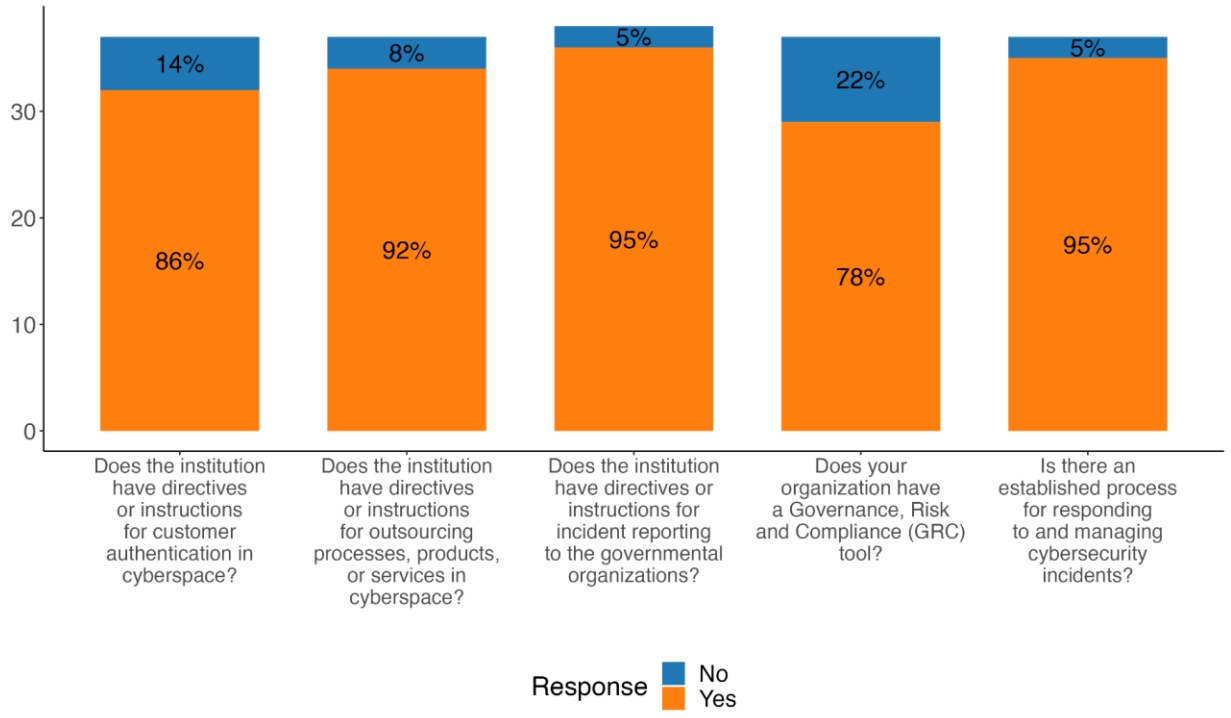

Figure 11. Responses about operations and incident management?

The stacked bar chart (Figure 11) provides insights into how institutions implement core cybersecurity governance practices. The x-axis lists five yes-or-no questions, and the y-axis shows the percentage of participants who answered "Yes" (orange) and "No" (blue) for each question. Below are the key observations:

- **Widespread Adoption of Essential Practices:**

  The graph reveals a positive trend, with most participants endorsing essential cybersecurity governance practices. Here's a breakdown:

  - **Customer Authentication:** The use of directives or instructions for customer authentication in cyberspace appears prevalent (over 85%), indicating measures to safeguard online customer interactions.
  - **Outsourcing Governance:** A considerable majority (over 90%) of institutions have directives or instructions for outsourcing processes, products, or services in cyberspace. This suggests a focus on managing cybersecurity risks associated with third-party vendors.

- **Incident Reporting:** A significant portion (over 90%) of participants reported having directives or instructions for reporting cybersecurity incidents to government organizations. This suggests adherence to regulatory requirements and a commitment to information sharing.
- **Incident Response:** Nearly all (95%) of institutions indicated having an established process for responding to and managing cybersecurity incidents. This highlights a strong focus on preparedness for potential cyberattacks.
- **Governance, Risk, and Compliance (GRC) Tools:** While the adoption of GRC tools appears positive (over 75%), there's room for improvement compared to other practices. GRC tools can streamline risk management, compliance, and overall cybersecurity governance.

Areas for Potential Improvement:

- **Enhancing GRC Tool Adoption:** Encouraging wider adoption of GRC tools could lead to more efficient and centralized management of cybersecurity governance processes.

Additional Considerations:

- **Understanding Category Variations:** It would be insightful to analyze the data while considering the category of each institution (refer to previous analysis for category details). This could reveal variations in practice adoption across different categories.
- **Standardization and Best Practices:** Further research into industry best practices and standardized frameworks for cybersecurity governance could provide valuable benchmarks for improvement.

6.7 Performance evaluation and continual improvement

This section explores how institutions across different categories evaluate the effectiveness of their cybersecurity measures. The survey included two questions on this topic. Figure 12 focuses on the primary methods used for monitoring and evaluation. Referring to figure 12, we observe that institutions in Category 1 demonstrate a strong commitment to comprehensive cybersecurity evaluation. As shown in Figure 12, a very high percentage (86%) of participants in this category endorse the use of all the standard methods for monitoring and evaluation. This suggests a rigorous approach to measuring cybersecurity effectiveness in Category 1.

Furthermore, the graph indicates that the percentage of institutions using all standard methods for monitoring and evaluation is lower in Categories 2 through 5. This may suggest a need for improvement in performance evaluation practices within these categories.

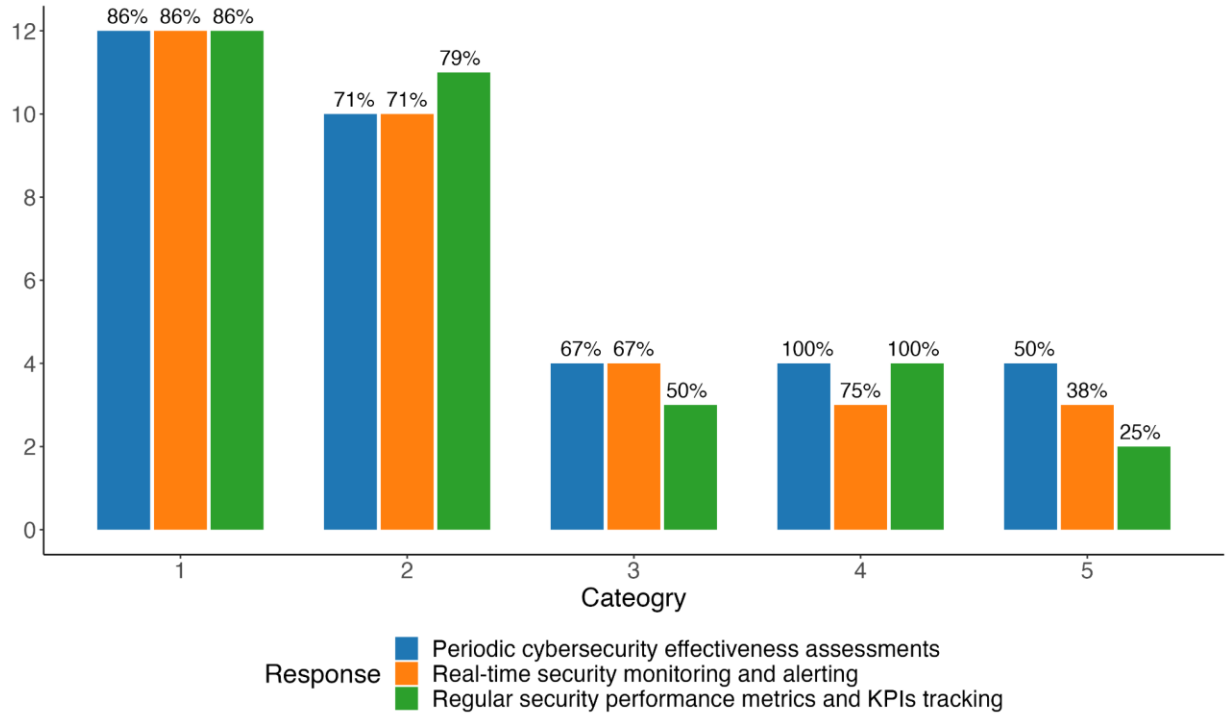

Figure 12. Methods used for monitoring and evaluation of the cybersecurity measures effectiveness

6.8 Compliance and legal requirement

This section delves into the methods institutions employ to stay up-to-date with and adhere to legal and regulatory requirements for cybersecurity. A very high percentage (almost all) of institutions in Category 1 have indicated that they have procedures in place for ensuring compliance with cybersecurity regulations, as shown in the top-left bar chart of Figure 13. This highlights the universal commitment to staying informed about the evolving cybersecurity landscape. The compliance rates for Categories 2, 3, 4, and 5 appear to be lower than Category 1, based on the shorter bars in the graph. There's a possibility that these categories may have resource constraints that influence their approach to regulatory compliance.

As for the adoption of cybersecurity insurance by the organizations, the graph (top-right) reveals a clear difference in cyber insurance adoption across different categories. Category 1 has the highest adoption rate (90%), followed by Category 2 (73%) and Category 3 (55%). Several factors could explain the variations in cyber insurance adoption across categories, including risk profile, resource constraints, and awareness.

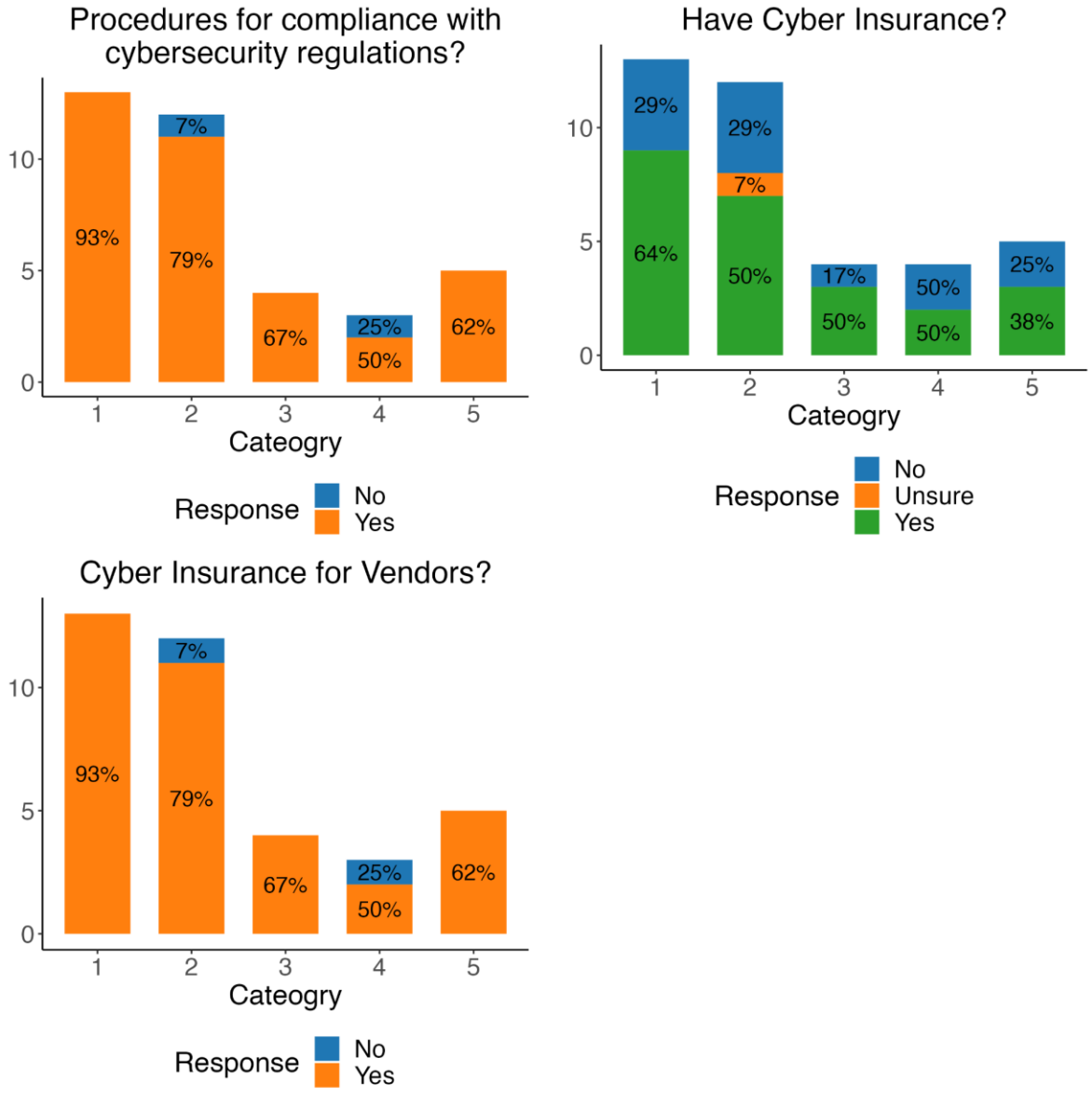

Figure 13. Responses to the questions about compliance with legal requirements

The bottom-left graph sheds light on the practices of institutions from different categories regarding cyber insurance requirements for their vendors. There appears to be a difference in how institutions from various categories approach vendor cyber insurance requirements.

Institutions in Category 1 exhibit the most stringent approach, as reflected by a potentially high bar in the graph. This suggests they prioritize vendor cyber insurance as a risk mitigation strategy. The bars for Categories 2, 3, 4, and 5 appear to be shorter than Category 1. This indicates a potential mix of practices within these categories. Some institutions might require vendor cyber insurance, while others may not.

6.9 Concluding Thoughts

This section summarizes the key insights gleaned from the concluding questions of the questionnaire. Participants were asked to briefly describe their organization's strongest aspect of cybersecurity governance and the challenges they face in improving it.

At the end of the questionnaire, we ask participants to briefly describe the strongest aspect of their organization’s cybersecurity governance and what challenges their organization face in improving cybersecurity governance.

Strongest Aspects:

- **Management Support:** A recurring theme emerged – strong support from top management was frequently cited as a key strength. This highlights the critical role of leadership buy-in for effective cybersecurity governance.
- **Established Cybersecurity Organization:** Many participants identified a well-established cybersecurity organization within their institution as a significant strength. This suggests a focus on dedicated structures and resources for managing cybersecurity.

Challenges:

- **Cybersecurity Landscape Complexity:** The rapidly growing complexity of the cybersecurity landscape was a frequently mentioned challenge. Institutions are likely grappling with keeping pace with evolving threats and vulnerabilities.
- **Skilled Workforce Shortage:** The shortage of skilled cybersecurity professionals was another common concern. This highlights the need for strategies to address the talent gap in the cybersecurity field.

These findings suggest that providing the necessary infrastructure for skilled human resource training and retention is crucial for strengthening cybersecurity governance within banking and financial institutions. This could encompass initiatives like training programs, competitive compensation packages, and fostering a culture of continuous learning in cybersecurity.

7. Summary and Conclusion

A literature survey about the cybersecurity considerations in financial institutes in USA, Europe and China, as the world largest economies, was presented in the section two. Regulatory infrastructures, organizations and requirements in these three economic powers have been briefly discussed based on the available online data. It is clear that the implementation of cybersecurity frameworks and standards in the banking and financial institutions are strongly recommended by the national institutes to meet the regulatory requirements and to be safe against cyberattacks.

This article explores cybersecurity considerations in banking and financial institutions across major economic regions – the United States, Europe, and China. Section two provides a brief overview of the regulatory landscape in these regions, highlighting the importance of cybersecurity governance and standards for banking and financial institutions.

The remaining sections investigated the current state of cybersecurity governance within banking and financial institutions.

A survey was conducted with 46 participants, including 30 from GCC countries and 16 from others. The analysis compares and contrasts responses across predefined categories (based on the cybersecurity framework adopted by the organizations), offering insights into how institutions implement their cybersecurity governance. Here are some of the key findings:

- **Maturity Gap:** Over 63% of respondents perceive a gap between their current cybersecurity posture and their desired maturity level, indicating a need for improvement.
- **Centralized Cybersecurity Governance:** A significant majority across most categories favor a centralized approach with a dedicated cybersecurity team, highlighting a preference for centralized structures.

- **Stakeholder Engagement:** While all Category 1 institutions actively identify and meet stakeholder requirements, a disparity exists in Categories 2-5.
- **Strategic Alignment:** All but two respondents reported alignment of cybersecurity efforts with overall strategic direction, reflecting growing recognition of cybersecurity's importance.
- **Strong Cybersecurity Culture:** Nearly 90% of participants reported buy-in from all business units for the cybersecurity strategy, indicating a strong security culture.
- **Risk Management Approaches:**
    - Conducting regular risk assessments is the most prevalent method.
    - Many institutions leverage established frameworks (e.g., ITAR, NIST, AMF) for risk management.
    - Cross-functional team involvement is another key strategy.
    - All but two institutions maintain records of cybersecurity risks and their treatment.
    - Nearly 90% consider all critical factors during risk assessments.
- **Cybersecurity Budget Allocation:** Category 1 institutions dedicate a significantly larger portion of their IT budget to cybersecurity compared to others. This may reflect a higher risk profile or different resource optimization strategies in other categories.
- **Resource Adequacy:** Technological tools received the highest endorsement for resource adequacy across all categories.
- **Operational Control:**
    - Category 1 institutions leverage a comprehensive approach combining regular reviews, policy implementation, and automation.
    - Categories 2 and 4 also demonstrate a strong emphasis on operational control.
    - Categories 3 and 5 seem to rely more heavily on regular security audits and assessments.
- **Monitoring and Evaluation:** Category 1 institutions use a wider range of standard methods for monitoring and evaluation compared to other categories, except Category 4 which utilizes all standard methods.

- **Regulatory Compliance:** All participants in Categories 1, 3, and 5, and most in others, have procedures for ensuring regulatory compliance, demonstrating a focus on legal requirements.
- **Strongest Aspects of Cybersecurity Governance:** Top management support and a well-established cybersecurity organization emerged as the most frequently cited strengths.
- **Challenges:** Rapidly evolving cybersecurity threats and a shortage of skilled personnel were the most frequently mentioned challenges hindering cybersecurity governance improvement.

The survey findings highlight the importance of continuous improvement in cybersecurity governance for banking and financial institutions.

Addressing the skills gap through training and retention programs is crucial. Additionally, fostering a culture of strong stakeholder engagement, risk management, and ongoing monitoring are essential for enhancing cybersecurity posture. This paper emphasizes the need for ongoing efforts by banking and financial institutions to adapt to the ever-changing cybersecurity landscape and maintain robust governance practices.

This study illustrates the growing importance of centralized cybersecurity governance in financial organizations, where the CISO works closely with legal, compliance, risk, and audit teams to ensure a comprehensive cyber-risk management framework. Utilizing tools like the RACI matrix and adhering to the Three-Lines-of-Defense model, banking and financial institutions can enhance their resilience against cyber threats by clearly defining roles and responsibilities across the organization.

By adopting these best practices, banking and financial institutions can ensure that cybersecurity is not just an IT issue but a critical component of their overall governance and risk management strategies.

7.1 Limitations and future work

The survey employed in this study primarily focuses on evaluating the cybersecurity governance frameworks within banking and financial institutions. Future iterations of this research could integrate the following dimensions to provide a more holistic analysis of cybersecurity governance:

1. **Board and Senior Management Involvement:**
   A key element of effective cybersecurity governance is the involvement of the board of directors and senior management. According to studies, organizations with active board oversight of cybersecurity are more likely to have robust security postures. The survey did not explicitly assess the degree of board-level engagement, and future research should include questions on how involved senior leadership is in setting cybersecurity strategies, approving budgets, and overseeing risk management activities related to cyber threats.
2. **Role of Internal Audit in Cybersecurity Governance:**
   Internal audit functions play a critical role in providing independent assurance over an organization's cybersecurity governance. A growing number of banking and financial institutions involve internal audit in the review of cybersecurity practices to ensure compliance with regulations and alignment with strategic objectives. The absence of this element in the survey limits the scope of the study's conclusions.

By incorporating these elements in future surveys, a more comprehensive understanding of cybersecurity governance can be achieved. Each of these aspects contributes to a well-rounded cybersecurity governance framework and has been recognized as crucial for the protection of banking and financial institutions.

References

1. European Central Bank. (2018, December). *Cyber resilience oversight expectations for financial market infrastructures*.
2. Financial Stability Institute. (2017, August). *FSI Insights on policy implementation, No. 2: Regulatory approaches to enhance banks' cyber-security frameworks*.
3. Financial Services Sector Coordinating Council. (2015). *Financial Services Sector specific plan*.
4. European Commission. (2018). *FinTech Action plan: For a more competitive and innovative European financial sector*.
5. GTG. (n.d.). Financial services and fintech updates 10/10. Retrieved from: https://gtg.com.mt/financial-services-and-fintech-updates-10-10.
6. Tech.mt. (n.d.). The priority areas of the digital finance strategy by the EU commission. Retrieved from: https://tech.mt/media/blog/the-priority-areas-of-the-digital-finance-strategy-by-the-eu-commission.
7. Regulatory Policy Development and Updates. (2015, March). *Cyber Security and the impact on banks in China*.
8. Cyber considerations for banking expansion into China. (2023).
9. Suša Vugec, D., & Spremić, M. (2017). IT governance adoption in banking and insurance sector: Longitudinal case study of COBIT use. *International Journal for Quality Research, 11*(3), 691–716.
10. Gartner Research. (2021-2022). Cybersecurity Organization Design Benchmarking Data. Gartner Inc.
11. Gartner Research. (2021). Sample Cybersecurity Organization Charts. Gartner Inc.
12. Scholtz, T. (2021). How to Design a Practical Security Organization. Gartner Inc.
13. Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.htm
14. European Central Bank. (2020). *Cyber Resilience Strategy for Financial Market Infrastructures*. European Central Bank. https://www.ecb.europa.eu/paym/pol/html/cyberresilience.en.html

15. Financial Stability Board. (2020). *Effective Practices for Cyber Incident Response and Recovery*. Financial Stability Board. https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery/
16. European Union. (2016). *General Data Protection Regulation (GDPR)*.
17. J.P. Morgan Chase. (2022). *Cybersecurity Investment and Risk Management*.
18. Deloitte. (2021). *Financial Services Industry Outlook: Cybersecurity*.
19. PwC. (2021). *Cybersecurity in Banking Survey*.
20. McKinsey & Company. (2020). *The Risk and Resilience of Digital Innovation in Banking*.
21. European Banking Authority. (2020). *Fintech Cybersecurity Governance Report*.
22. Gartner, Inc. (2023). CPS Security Governance — Best Practices From the Front Lines.
23. Gartner, Inc. (2023). Define Legal, Compliance, Risk and Audit Roles in Cyber-Risk Governance.
24. Financial Stability Board. (2009). FSB Principles for Sound Compensation Practices.
25. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004). Enterprise Risk Management—Integrated Framework.
26. Baldwin, C. (2016). Cyber Heist at Bangladesh Bank: How It Happened. Reuters. Retrieved from: https://www.reuters.com/article/us-usa-fed-bangladesh-swift-insight-idUSKCN0YB0DD
27. SWIFT. (2016). Customer Security Programme (CSP).
28. Europol. (2017). WannaCry Ransomware Attack. Retrieved from: https://www.europol.europa.eu/media-press/newsroom/news/wannacry-ransomware-recent-cyber-attack
29. Federal Trade Commission. (2019). Equifax Data Breach Settlement. Retrieved from https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
30. PricewaterhouseCoopers. (2018). The Global State of Information Security Survey 2018.
31. National Association of Corporate Directors. (2017). Cyber-Risk Oversight Handbook.
32. European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union, L119, 1–88.

33. Gartner. (2018). Integrating Cybersecurity into Enterprise Risk Management.
34. Central Bank of Kuwait Cybersecurity Framework – CBK Documentation.
35. Saudi Central Bank Cybersecurity Regulations – SAMA Regulatory Framework.
36. Central Bank of the UAE Cybersecurity Regulations – Banking and Financial Institutions Guidelines.
37. Qatar Central Bank Cybersecurity Strategy – QCB Regulatory Guidelines.
38. Joint Statement on the EU - U.S. Joint Financial Regulatory Forum: Retrieved from: https://home.treasury.gov/news/press-releases/jy0386
39. CBO issues Regulatory Framework of Cyber Security and Resilience. Retrived from: https://www.thearabianstories.com/2023/09/20/cbo-issues-regulatory-framework-of-cyber-security-and-resilience
40. Central Bank of Bahrain Cybersecurity Risk Management
41. World Bank Group - Cybersecurity. Retrieved from: https://www.worldbank.org/en/topic/digital/brief/cybersecurity

CYBER GUARD: A COMPREHENSIVE GUIDE TO EFFECTIVE GOVERNANCE

Table of Contents

Introduction 49

Scope 49

Audience 49

Section1: Organizational Cybersecurity Context 49

1.1 Cybersecurity Management Framework 50

1.2 Distribution of Cybersecurity Responsibilities 52

Section 2: Leadership, Commitment, and Cybersecurity Culture 52

2.1 Commitment of Top Management to Cybersecurity Governance 53

2.3 Training 54

2.4 Cybersecurity Culture 55

Section 3: Planning and Risk Management 55

3.1 Identifying and Prioritizing Cybersecurity Risks 56

3.2 Cybersecurity Risk Management Plan 56

3.3 Cybersecurity Database 57

3.4 Risk Strategy Factors 58

Section 4: Support and Resources 58

4.1 Resources for Implementing and Maintaining Cybersecurity Measures 59

Section 5: Operations and Incident Management 60

5.1 Managing Operational Processes Related to Cybersecurity 60

5.2 Governance, Risk, and Compliance (GRC) tools 61

5.2 Tracking Cyber Breaches 61

5.3 Incident Response Process 62

5.4 Incident Reporting to the Governmental Organizations 63

5.5 Customer Authentication 63

5.6 Outsourcing Processes, Products, or Services 64

Section 6: Performance Evaluation and Continual Improvement 65

6.1 Monitoring and Evaluating the Effectiveness of Cybersecurity Measures 65

Section 7: Compliance and Legal Requirements 66

7.1 Established Procedures for Compliance with Cybersecurity Laws and Regulations 67

7.2 Cyber Insurance 67

7.2 Cyber Insurance During Vendor Selection 68

7.3 Third-Party Risk Management (TPRM) **69**
7.4 Staying up-to-date to Monitor and Respond to Regulatory Updates **70**

---

8. Introduction

Welcome to the Cybersecurity Governance Manual, a comprehensive guide designed to empower organizations in navigating the complex landscape of cybersecurity governance. In today's digital age, the protection of sensitive information, critical assets, and organizational integrity against evolving cyber threats is paramount. This manual serves as a roadmap for organizations seeking to establish robust cybersecurity governance frameworks, mitigate risks, and foster a culture of resilience.

Scope

Covering a wide array of topics ranging from the organizational cybersecurity context to compliance and legal requirements, each section delves into key components essential for effective cybersecurity governance. By offering a comprehensive guide filled with actionable insights and guidelines, this manual equips organizations in the banking and financial sector with the tools they need to bolster their cybersecurity posture.

By exploring crucial areas such as leadership commitment, planning and risk management, support and resources, operations and incident management, performance evaluation, and compliance with legal requirements, organizations can develop holistic cybersecurity strategies tailored to their unique needs and challenges. Additionally, this manual emphasizes the importance of continual improvement, adaptability, and staying abreast of regulatory changes to maintain resilience in the face of evolving cyber threats.

Audience

Whether you are a cybersecurity professional, an organizational leader, or an individual responsible for cybersecurity governance, this manual equips you with the knowledge and tools necessary to navigate the ever-changing cybersecurity landscape with confidence and efficacy.

9. Section1: Organizational Cybersecurity Context

Within the realm of cybersecurity governance, understanding the organizational landscape is crucial. This section delves into pivotal elements essential for establishing a robust cybersecurity framework within organizations. By exploring the adoption of recognized cybersecurity management frameworks, the structure of cybersecurity teams, and the identification of key stakeholders, organizations can gain invaluable insights. These insights not only bolster the organization's cybersecurity posture but also ensure alignment with industry standards and best practices. Moreover, by addressing stakeholder requirements, organizations foster trust, transparency, and collaboration, thus fortifying their resilience against evolving cyber threats. This section serves as a foundational guide, empowering organizations to navigate the complex cybersecurity landscape.

1.1 Cybersecurity Management Framework

A cybersecurity framework is a structured set of documents that provides guidelines, standards, and best practices for managing cybersecurity risks. These frameworks are designed to help organizations reduce their exposure to vulnerabilities and weaknesses that hackers and other cybercriminals may exploit.

Here are some key points about cybersecurity frameworks:

1. **Purpose**: Cybersecurity frameworks exist to enhance an organization's security posture by offering guidance on risk management. They help organizations establish effective security practices and protect their digital assets.
    - **Other Industry-Specific Frameworks**: Different industries (such as finance, healthcare, and critical infrastructure) have their own specialized frameworks.
    - **International Standards**: ISO/IEC 27001 and ISO/IEC 27002 are globally recognized standards for information security management.
2. **Benefits**:
    - **Risk Reduction**: By following a framework, organizations can systematically address vulnerabilities and minimize risks.
    - **Consistency**: Frameworks promote consistent security practices across an organization.
    - **Compliance**: Many frameworks align with legal and regulatory requirements.
    - **Communication**: Frameworks facilitate communication about security practices among stakeholders.

There are various cybersecurity frameworks, each tailored to different needs and contexts. Some well-known frameworks include:

1. **ISO/IEC 27000**:
    - Widely considered the baseline for information security management systems (ISMS).
    - Focuses on the three pillars of cybersecurity: confidentiality, integrity, and availability (the CIA Triad).
    - Provides guidelines to keep an organization's data safe.
2. **NIST Cybersecurity Framework**:
    - Established by the National Institute of Standards and Technology (NIST).
    - Widely used by American companies.
    - Offers detailed guidance on risk assessment, continuous monitoring, incidence response, and awareness training.
    - Available in various versions to meet industry-specific needs.
3. **COBIT (Control Objectives for Information and Related Technologies)**:
    - Developed by ISACA (Information Systems Audit and Control Association).
    - Focuses on governance and management of enterprise IT.
    - Provides a comprehensive framework for aligning IT with business goals.
    - Useful for managing risks and ensuring compliance in the banking and financial sector.
4. **CIS Controls (Center for Internet Security Controls)**:
    - A set of 20 critical security controls designed to enhance cybersecurity.
    - Cross-compatible with other standards like PCI DSS, GDPR, HIPAA, and ISO 27001.
    - Strives for increased cybersecurity across the board.
    - Offers practical implementation tiers.

Useful resources:

https://www.splunk.com/en_us/blog/learn/cybersecurity-frameworks.html

https://omnistruct.com/nist-iso-cis-or-cobit-comparing-comprehensive-cybersecurity-frameworks/

https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

https://carbidesecure.com/resources/differences-and-similarities-between-nist-and-cis/

https://techbullion.com/cybersecurity-frameworks-a-guide-to-choosing-the-right-one-for-your-organization

1.2 Distribution of Cybersecurity Responsibilities

As organizations navigate the complexities of safeguarding sensitive financial data, they must carefully consider how to distribute cybersecurity responsibilities. Two primary models emerge: centralized and distributed:

- **Centralized Responsibility with a Dedicated Cybersecurity Team**: In this model, a specific team within the organization is solely responsible for cybersecurity. They handle all aspects of security, including monitoring, incident response, and vulnerability management. This approach ensures a focused and specialized effort to safeguard sensitive financial data.
- **Distributed Responsibility Across All Departments**: Alternatively, some organizations choose to distribute cybersecurity responsibilities across various departments. Each department takes ownership of security within its domain. While this approach promotes a sense of collective responsibility, it requires strong coordination and communication to ensure consistent security practices across the organization.

Given the critical nature of financial data and the constantly evolving threat landscape, a combination of both approaches is often advisable.

Useful resources:

https://blog.rsisecurity.com/financial-cybersecurity-best-practices-for-financial-services-organizations/

https://orbitingweb.com/blog/cybersecurity-best-practices-for-financial-institutions/

https://stefanini.com/en/insights/articles/the-role-of-cybersecurity-in-financial-services

10. Section 2: Leadership, Commitment, and Cybersecurity Culture

Building a fortress against cyber threats requires strong leadership, unwavering commitment, and a vibrant cybersecurity culture. This section dives deep into the key ingredients for fostering these essential pillars within the organization.

Through an exploration of the critical components related to leadership and cybersecurity culture, this section serves as a foundational guide, empowering organizations to cultivate strong leadership,

unwavering commitment, and a thriving cybersecurity culture, thereby enhancing their resilience in the face of evolving cyber threats.

2.1 Commitment of Top Management to Cybersecurity Governance

In the dominion of cybersecurity governance, organizations struggle with defining the roles and responsibilities regarding policy endorsement, resource allocation, and direct involvement in cybersecurity initiatives. Two primary strategies emerge: one emphasizing the endorsement of cybersecurity policies, while the other prioritizes the allocation of dedicated resources and direct involvement in initiatives. Each approach carries distinct implications for organizational cybersecurity readiness and resilience.

- **Endorsement of Cybersecurity Policies**: This involves the top management publicly supporting and advocating for the organization's cybersecurity policies. It demonstrates their commitment to security and sets the tone for the entire organization.
- **Allocation of Dedicated Resources for Cybersecurity**: When top management allocates specific resources (such as budget, personnel, or technology) exclusively for cybersecurity efforts, it shows a tangible commitment to protecting the organization's digital assets.
- **Direct Involvement in Cybersecurity Initiatives**: When top management actively participates in cybersecurity initiatives, such as attending security briefings, reviewing incident reports, or engaging with the security team, it reinforces the importance of security at all levels.

Useful resources:

https://blog.rsisecurity.com/financial-cybersecurity-best-practices-for-financial-services-organizations/

https://www.icaew.com/-/media/corporate/files/technical/corporate-finance/guidelines/cyber-security-in-corporate-finance-2024.ashx?la=en

https://fbijohn.com/best-cybersecurity-frameworks-financial-institutions/

https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf

2.2 Alignment of Cybersecurity Policies and Objectives with the Strategic Direction of the Organization

In cybersecurity governance within the banking and financial sector, organizations face the critical task of

aligning cybersecurity policies and objectives with the strategic direction. This alignment ensures that cybersecurity efforts integrate seamlessly with broader organizational goals, crucial for safeguarding sensitive financial data and maintaining the trust of stakeholders.

When considering the alignment of cybersecurity policies and objectives with the strategic direction of an organization, it is crucial to recognize that cybersecurity is not merely a technical issue; it is fundamentally a business problem.

When cybersecurity aligns with business goals, it becomes an integral part of the organizational culture. This alignment allows for effective risk management, better communication between IT professionals and C-suite executives, and the ability to demonstrate the net business impact of security risks.

On the other hand, if cybersecurity policies and objectives are not aligned with the strategic direction, it can lead to risks being overlooked. Poor communication between IT professionals and executives may result in security concerns flying under the radar until a major incident occurs. To avoid this, organizations should actively work toward alignment.

Useful resources:
https://www.weforum.org/agenda/2022/06/cybersecurity-protect-your-business/

2.3 Training

In the banking and financial sector, cybersecurity training for employees is crucial for safeguarding sensitive data. The frequency of training sessions directly impacts the organization's resilience against cyber threats. When deciding on the frequency of these trainings, organizations should follow the following instructions:

- **Annually**: Providing cybersecurity training once a year ensures that employees receive consistent and up-to-date information about security threats, best practices, and protocols. However, given the rapidly evolving nature of cyber threats, annual training might not be frequent enough to address emerging risks effectively.
- **Biannually**: Offering training twice a year strikes a balance between regular updates and practicality. It allows employees to stay informed without overwhelming their schedules. Biannual

training can cover essential topics such as phishing awareness, data protection, and incident response.

- **Quarterly**: Quarterly training provides a more proactive approach. It ensures that employees receive timely information about new threats, security policies, and compliance requirements. Frequent training sessions help reinforce good security habits and keep employees vigilant.

2.4 Cybersecurity Culture

Evaluating the effectiveness of cybersecurity culture is essential for protecting sensitive data. Various methods, such as employee feedback surveys, compliance audit results, and incident response effectiveness, are employed for assessment. These approaches offer valuable insights into different aspects of cybersecurity readiness.

- **Employee Feedback Surveys**: Gathering feedback directly from employees is essential. Regular surveys can help assess their awareness, understanding, and adherence to cybersecurity practices. It provides insights into how well the culture is embedded and identifies areas for improvement.
- **Compliance Audit Results**: Regular compliance audits evaluate whether your organization adheres to established security policies, procedures, and regulatory requirements. These results indicate the effectiveness of your cybersecurity practices and highlight any gaps or non-compliance.
- **Incident Response and Resolution Effectiveness**: Evaluating how well your organization responds to and resolves security incidents is critical. This includes assessing incident detection, containment, mitigation, and recovery processes. Effective incident response demonstrates a robust cybersecurity culture.

A comprehensive approach that combines employee feedback surveys, compliance audit results, and incident response effectiveness provides a holistic view of your organization's cybersecurity culture. Each of these practices contributes to building a resilient and security-conscious environment.

Useful resources:

https://www.forbes.com/sites/forbestechcouncil/2022/09/13/building-a-cybersecurity-culture-in-your-organization/?sh=6914e5a647a9

11.Section 3: Planning and Risk Management

The ever-shifting terrain of cybersecurity threats demands meticulous planning and robust risk management. This section equips you with the essential tools to navigate this complex landscape. By

exploring the core components of risk management, you'll gain the knowledge to develop a powerful defense system, fortifying your organization's resilience against ever-evolving cyberattacks.

3.1 Identifying and Prioritizing Cybersecurity Risks

For banking and financial institutions, pinpointing and prioritizing cybersecurity threats is the cornerstone of safeguarding sensitive data. Organizations employ various methods for this, including regular risk assessment exercises, the use of established risk management frameworks like FAIR or NIST RMF, and involving cross-functional teams. By combining these approaches, banking and financial institutions can construct a comprehensive defense system to neutralize potential threats and bolster their cybersecurity resilience.

Useful resources:

https://www.forbes.com/sites/forbestechcouncil/2022/09/13/building-a-cybersecurity-culture-in-your-organization/?sh=42cf55e747a9

https://www.cyberpilot.io/cyberpilot-blog/the-ultimate-guide-to-a-strong-security-culture

https://www.infosecurity-magazine.com/opinions/steps-positive-security-culture/

https://thrivedx.com/resources/article/the-role-of-culture-in-cybersecurity

3.2 Cybersecurity Risk Management Plan

Within the banking and financial sector, strict adherence to regulatory compliance necessitates a robust cybersecurity risk management plan. Such a plan plays a vital role in mitigating threats and safeguarding sensitive data. Banking and financial institutions leverage a diverse set of strategies to ensure the effectiveness of their risk management plans. This includes conducting regular compliance audits to assess adherence to regulations, involving dedicated legal and compliance teams in cybersecurity initiatives, and utilizing compliance management software to streamline processes. These approaches ensure a robust cybersecurity posture, enhancing resilience against cyber threats, laying a solid foundation for the implementation of key cybersecurity measures outlined in the following sections. We will explore some of these items in more detail later.

- **Implement an enterprise security framework**: Having a well-defined security framework ensures consistency and alignment across the organization. It provides a structured approach to managing risks and protecting sensitive data.

- **Create a culture fostering cybersecurity**: Cultivating a security-conscious culture is essential. Regular training, awareness programs, and emphasizing the importance of security among employees contribute to a robust cybersecurity posture.
- **Threat monitoring**: Continuously monitor for potential threats and vulnerabilities. Implement intrusion detection systems, security information and event management (SIEM) tools, and real-time monitoring to detect and respond promptly to any security incidents.
- **Vulnerability management**: Regularly assess and address vulnerabilities in your systems and applications. Patch management, vulnerability scanning, and penetration testing are critical components of effective vulnerability management.
- **Third-party risk management**: Banking and financial institutions often rely on third-party vendors. Assess the cybersecurity practices of these vendors thoroughly. Ensure they meet your security standards and have robust risk management processes in place.
- **Backup data**: Regularly back up critical data and systems. Having reliable backups ensures business continuity in case of cyber incidents or data breaches.
- **Incident response**: Develop a comprehensive incident response plan. This plan should outline steps to take when a security incident occurs, including communication protocols, containment measures, and recovery procedures.

Remember that cybersecurity is an ongoing process, and staying informed about emerging threats and adapting your practices accordingly is crucial.

Useful resources:

https://blog.rsisecurity.com/financial-cybersecurity-best-practices-for-financial-services-organizations/

https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf

https://online.hbs.edu/blog/post/risk-management

https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/value-and-resilience-through-better-risk-management

https://academic.oup.com/rfs/article-abstract/36/1/351/6585907?redirectedFrom=fulltext

https://link.springer.com/book/10.1007/978-1-4842-4194-3

https://www.afi-global.org/sites/default/files/publications/2019-11/AFI_GN37_DFS_AW_digital_0.pdf

3.3 Cybersecurity Database

Having a document or database on cybersecurity risk experience and treatment methods allows institutions to learn from past experiences, track trends, and implement effective risk mitigation strategies. Such

documentation enhances transparency, facilitates informed decision-making, and ensures compliance with regulatory requirements.

On the other hand, a lack of documented cybersecurity risk experience and treatment methods can be detrimental. Without proper records, an organization may struggle to address emerging threats, respond to incidents, or learn from past mistakes. It is advisable for banking and financial institutions to actively maintain and update their knowledge base related to cybersecurity risks.

Useful resources:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1303.ipd.pdf

https://hyperproof.io/resource/cybersecurity-risk-management-process/

https://www.imperva.com/learn/data-security/cybersecurity-risk-management/

3.4 Risk Strategy Factors

When planning for risk strategy, organizations weigh several crucial factors to ensure comprehensive risk management. Some of the important factors to consider are the classification of data, evaluation of asset value, assessment of potential financial impact, and consideration of reputational damage.

- **Classification of data**: This involves categorizing data based on its sensitivity and criticality. It helps determine appropriate security measures and access controls.
- **Asset value**: Assessing the value of assets (such as financial instruments, customer data, or intellectual property) is crucial. High-value assets may require stronger protection.
- **Financial impact**: Organizations analyze potential financial losses resulting from risks. Understanding the impact helps prioritize risk mitigation efforts.
- **Reputational damage**: Reputation is vital in the financial industry. Negative publicity can lead to loss of trust, customers, and business opportunities.

A comprehensive risk strategy should address all the above-mentioned factors.

12.

13.Section 4: Support and Resources

In the realm of cybersecurity governance, adequate support and resources are fundamental pillars for effective implementation and maintenance of cybersecurity measures. This section covers the crucial aspects of support and resource allocation essential for fortifying organizational resilience against cyber threats.

By examining the key aspects that will be covered in this section, organizations can evaluate the adequacy of their current cybersecurity support and resource allocation within their overall framework. This evaluation helps identify areas for improvement, allowing organizations to take proactive measures and strengthen their cybersecurity posture. By effectively allocating resources and providing sufficient support, organizations can increase their resilience against cyber threats, ultimately navigating the ever-changing cybersecurity landscape with greater confidence.

4.1 Resources for Implementing and Maintaining Cybersecurity Measures

Securing the required resources to fortify cybersecurity defenses is a top priority for organizations operating in the dynamic landscape of the banking and financial sector. This necessitates securing resources across three key categories: staffing, technology, and budget.

1. **Staffing**: Having a skilled and adequate cybersecurity workforce is essential. Trained professionals can monitor systems, respond to incidents, and ensure compliance with security policies.
2. **Technological Tools**: Leveraging advanced tools and technologies is vital. These include intrusion detection systems, firewalls, encryption, and security information and event management (SIEM) solutions. Investing in robust technological tools enhances the organization's ability to detect, prevent, and mitigate cyber threats.
3. **Financial Resources**: Adequate funding is necessary for cybersecurity initiatives. It supports infrastructure upgrades, training programs, risk assessments, and ongoing monitoring. Without sufficient financial resources, organizations may struggle to maintain effective cybersecurity practices.

Useful resources:

https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf

https://www.ekransystem.com/en/blog/banking-and-financial-cyber-security-compliance

https://blog.rsisecurity.com/financial-cybersecurity-best-practices-for-financial-services-organizations/

14.Section 5: Operations and Incident Management

Effective Operations and Incident Management act as the bedrock of a resilient cybersecurity framework. This section dives deep into the essential components for controlling security operations and efficiently managing cyber incidents. By mastering these critical aspects, organizations can significantly bolster their overall resilience against cyber threats.

5.1 Managing Operational Processes Related to Cybersecurity

Navigating the complex terrain of the banking and financial sector requires adept control and management of operational processes related to cybersecurity. Ensuring the security of sensitive data and upholding trust are fundamental in this dynamic environment. To achieve this, organizations employ a range of strategies, including implementing formal cybersecurity policies and procedures, utilizing automated cybersecurity tools and technologies, and conducting regular security audits and assessments. By integrating these approaches, banking and financial institutions can proactively manage operational processes related to cybersecurity, thereby enhancing resilience against potential threats.

- **Implementation of formal cybersecurity policies and procedures**: This is a crucial step. Having well-defined and documented policies ensures that everyone in the organization understands their roles and responsibilities regarding cybersecurity. It helps establish a consistent approach to security across the organization.
- **Use of automated cybersecurity tools and technologies**: Automation plays a significant role in enhancing security. Automated tools can continuously monitor systems, detect anomalies, and respond to threats promptly. Examples include intrusion detection systems, firewalls, and security information and event management (SIEM) solutions.
- **Regular security audits and assessments**: Regular audits and assessments are essential for evaluating the effectiveness of security controls. They help identify vulnerabilities, assess compliance with policies, and ensure that security measures are up to date.

Useful resources:

https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf
https://blog.rsisecurity.com/financial-cybersecurity-best-practices-for-financial-services-organizations/
https://www.gartner.com/smarterwithgartner/the-cfo-cybersecurity-risk-checklist
https://builtin.com/cybersecurity/cybersecurity-banking-financial-services

5.2 Governance, Risk, and Compliance (GRC) tools

Governance, Risk, and Compliance (GRC) tools provide a centralized hub for managing your organization's security posture. These tools streamline processes by offering a single platform to manage governance policies, assess risks, and monitor compliance with regulations. By leveraging GRC tools, organizations gain greater visibility into potential risks, enabling informed decision-making. This translates to a more proactive approach to risk management, ensuring regulatory compliance, and upholding strong governance practices.

Useful resources:
https://blog.rsisecurity.com/grc-in-the-banking-industry-financial-services/
https://thedigitalprojectmanager.com/tools/grc-tools/

5.2 Tracking Cyber Breaches

The ever-shifting threat landscape of the banking and financial sector demands constant vigilance against cyber breaches. To identify and mitigate these incidents promptly, organizations rely on a robust tracking strategy. This often involves a combination of methods:

- **Detailed Incident Response Logs:** Maintaining detailed incident response logs is crucial. These logs capture information about security incidents, including breach attempts, their impact, and the actions taken to mitigate them. By analyzing these logs, organizations can identify patterns, assess the effectiveness of their response, and learn from past incidents.
- **Centralized GRC Tools:** Leveraging Governance, Risk, and Compliance (GRC) tools allows for centralized tracking and analysis of breach activity, offering a holistic view of potential threats.
- **Manual Tracking Methods:** Relying solely on manual tracking can be challenging and error prone. It may involve spreadsheets, emails, or other manual processes. While some level of manual tracking

is necessary, it should complement automated systems rather than replace them. Manual tracking alone may not be sufficient for timely detection and response to breaches.

Implementing a combination of automated tools and human vigilance ensures a proactive and effective approach to tracking cyber breaches in the banking and financial sector.

Useful resources:

https://www.iacis.org/iis/2021/1_iis_2021_63-74.pdf

https://www.forbes.com/sites/forbesfinancecouncil/2023/09/11/cybersecurity-in-finance-protecting-client-data-and-mitigating-risks/?sh=304b69763c51

https://www.cybersecuritydive.com/news/financial-services-malicious-cyber/700978/

https://www.bitsight.com/blog/financial-impact-cyber-attacks

5.3 Incident Response Process

The incident response process, as outlined by the leading security framework NIST (National Institute of Standards and Technology), consists of six clearly defined phases:

1. **Preparation**: This phase involves setting up the necessary infrastructure, policies, and procedures to handle incidents effectively. It includes creating incident response plans, assembling incident response teams, and establishing communication channels.
2. **Detection and Analysis**: During this phase, organizations actively monitor their systems for signs of potential incidents. When an incident occurs, it is detected, analyzed, and assessed to understand its impact and severity.
3. **Containment**: Once an incident is confirmed, the focus shifts to containing its spread. This involves isolating affected systems, preventing further damage, and minimizing the impact on critical assets.
4. **Eradication**: In this phase, organizations work to completely remove the threat from their systems. This may involve patching vulnerabilities, removing malware, or fixing misconfigurations.
5. **Recovery**: After eradicating the threat, the goal is to restore affected systems to normal operation. Organizations recover data, restore services, and verify that everything is functioning as expected.
6. **Post-Incident Activity**: Finally, organizations conduct a thorough review of the incident. Lessons learned are documented, and improvements are made to enhance future incident response efforts.

Banking and financial institutions follow this structured process to effectively respond to and manage cybersecurity incidents. It ensures a coordinated and efficient approach to safeguarding critical financial systems and data.

Useful resources:

https://www.subrosacyber.com/blog/incident-response-phases-in-cyber-security

https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf

https://www.fsb.org/wp-content/uploads/P191021.pdf

https://www.cyberwatching.eu/sites/default/files/Cyberwatching_CyberSec4Europe_IncidentReportingInTheFinancialSector.pdf

5.4 Incident Reporting to the Governmental Organizations

Banking and financial institutions often have directives and instructions in place for incident reporting to governmental organizations. These guidelines ensure timely communication and collaboration in case of cybersecurity incidents. For instance:

- The Cyber Incident Reporting for Critical Infrastructure Act (2022) mandates critical infrastructure companies to report significant cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours. It also requires firms to report ransomware payments within 24 hours.
- Additionally, the Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (2022) stipulate that banking organizations must notify their primary federal regulator when a computer-security incident occurs, causing harm to operations or customer services.

If an institution lacks such directives or instructions, it may face challenges in responding effectively to incidents and collaborating with relevant authorities.

5.5 Customer Authentication

The Federal Financial Institutions Examination Council (FFIEC) issued updated guidance titled "Authentication and Access to Financial Institution Services and Systems" in August 2021. This guidance provides examples of effective authentication and access risk management principles and practices for banking and financial institutions.

Here are the key points from the guidance:

1. **Risk Assessment**: Banking and financial institutions should conduct risk assessments to determine an effective authentication strategy based on the risks associated with various services available to online customers.
2. **Multi-Factor Authentication (MFA)**: Implement MFA to enhance security. MFA involves using multiple factors (such as passwords, biometrics, or tokens) to verify a user's identity.
3. **Layered Security Controls**: For consumer accounts, implement layered security controls. For business accounts, use controls consistent with the increased risk posed by business accounts.
4. **Principle of Least Privilege**: While provisioning access, establish the principle of least privilege. This means granting users only the minimum access necessary to perform their tasks.
5. **Monitoring and Logging**: Implement monitoring, activity logging, and reporting processes to track access and detect any suspicious activities.
6. **Secure Credential and API-Based Authentication**: Ensure secure credential management and use secure application programming interface (API)-based authentication.
7. **Secure Email Systems and Browsers**: Establish security controls to secure email systems and internet browsers.
8. **Customer Call Center and Help Desk Operations**: Implement secure processes for customer call centers and IT help desks, including robust customer and user identity verification.

Banking and financial institutions should prioritize risk assessment, layered security, and robust authentication practices to protect information systems, accounts, and data in cyberspace.

Useful resources:

https://www.mofo.com/resources/insights/210817-ffiec-issues-updated-guidance

https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-ffiec-guidance-on-authentication-and-access-to-financial-institution-services-and-systems-oct21.pdf

https://www.ffiec.gov/%5C//press/pdf/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf

5.6 Outsourcing Processes, Products, or Services

Banking and financial institutions should indeed have clear directives and guidelines for outsourcing activities. These instructions help manage risks associated with outsourcing and ensure compliance with regulatory requirements. For instance, the Reserve Bank of India (RBI) has issued Master Directions on Outsourcing of Information Technology Services for regulated entities. These directions emphasize the need for effective risk management, compliance, and governance in outsourcing arrangements.

Not having specific instructions can lead to uncontrolled risks, inadequate supervision, and potential harm to customers and the institution itself. Without proper guidelines, banking and financial institutions may struggle to maintain cybersecurity standards and protect sensitive data.

Useful resources:

https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12486

https://www.legal500.com/developments/thought-leadership/new-rbi-it-outsourcing-directions-and-key-takeaways-for-fintech-agreements/

https://www.upguard.com/blog/cybersecurity-regulations-financial-industry

https://blog.rsisecurity.com/financial-cybersecurity-best-practices-for-financial-services-organizations/

https://www.nelsonmullins.com/storage/67ff96a703bccfa7e47f358b634a8c17.pdf

15.

16. Section 6: Performance Evaluation and Continual Improvement

At the heart of any effective cybersecurity framework lies a commitment to continuous assessment and improvement. This section covers the critical elements essential for monitoring and enhancing the effectiveness of cybersecurity measures. By actively monitoring performance and fostering a culture of iterative refinement, organizations can build resilience against ever-evolving cyber threats and navigate the dynamic security landscape with confidence.

6.1 Monitoring and Evaluating the Effectiveness of Cybersecurity Measures

In the fast-paced world of finance, staying ahead of cyber threats requires more than just routine monitoring, it demands innovation and adaptability. Beyond routine monitoring, it requires innovative and adaptable cybersecurity strategies. A range of methods, like security metrics and periodic assessments, provide valuable insights into their security posture. By leveraging this diverse toolkit, banking and financial institutions can proactively fortify their defenses and navigate the ever-evolving cyber threat landscape with confidence.

We will explore these dynamic methods further to understand their collective impact on cybersecurity readiness within the banking and financial sector.

- **Regular Security Performance Metrics and KPIs Tracking**: This involves setting up key performance indicators (KPIs) related to security and consistently tracking them. Regularly measuring and analyzing these metrics helps organizations identify trends, assess the impact of security controls, and make informed decisions. It's a valuable practice for maintaining a proactive security posture.
- **Periodic Cybersecurity Effectiveness Assessments**: Conducting periodic assessments allows organizations to evaluate the overall effectiveness of their cybersecurity measures. These assessments may include vulnerability scans, penetration testing, and security audits. By periodically assessing the security landscape, organizations can identify gaps, prioritize improvements, and ensure alignment with industry standards and regulations.
- **Real-Time Security Monitoring and Alerting**: Real-time monitoring involves continuous surveillance of network traffic, system logs, and security events. When anomalies or potential threats are detected, alerts are triggered, enabling swift response and mitigation. Real-time monitoring is crucial for identifying and addressing security incidents promptly.

Useful resources:

https://blog.rsisecurity.com/financial-cybersecurity-best-practices-for-financial-services-organizations/

https://arcticwolf.com/resources/blog/seven-cybersecurity-best-practices/

https://orbitingweb.com/blog/cybersecurity-best-practices-for-financial-institutions/

https://www.fsmatters.com/Cyber-Security-in-the-Financial-Services-Sector

17.

18. Section 7: Compliance and Legal Requirements

A strong cybersecurity program necessitates adherence to the legal landscape. This section explores the key elements for ensuring an organization complies with relevant cybersecurity laws and regulations. By actively managing these legal requirements and proactively mitigating risks, organizations can strengthen their defenses and build trust in their digital operations.

7.1 Established Procedures for Compliance with Cybersecurity Laws and Regulations

When it comes to the banking and financial sector, ensuring compliance with relevant cybersecurity laws and regulations is crucial. These regulations are designed to protect sensitive financial data, prevent fraud, and maintain the integrity of financial systems.

Banking and financial institutions typically have robust security protocols, risk assessments, and regular audits to meet legal requirements. They must actively implement and maintain cybersecurity measures to safeguard their systems, customer data, and overall stability. Failing to comply with relevant regulations can result in severe consequences, including financial penalties and reputational damage.

7.2 Cyber Insurance

When it comes to the banking and financial sector and cyber insurance, there are several best practices to consider:

1. **Establish a Formal Cyber Insurance Risk Strategy**:
    - Obtain approval from senior management and the board of directors (or other governing body if there is no board of directors). Having a well-defined strategy ensures that cyber risks are adequately addressed.
2. **Manage and Eliminate Exposure to Silent Cyber Insurance Risk**:
    - Rewrite standard policies to explicitly state whether cyber incidents will be covered.
    - Consider purchasing reinsurance for contracts that include silent cyber insurance risks.
3. **Evaluate Systemic Risk**:
    - Understand which third-party vendors are used across multiple insureds.
    - Assess the potential impact of a catastrophic cyber incident on these third-party vendors.
4. **Rigorously Measure Insured Risk**:
    - Recognize that current cyber exposure may be underestimated relative to premiums charged.
    - Address systemic risk (such as vulnerabilities in common software) and silent cyber risks (losses from incidents not explicitly granting cyber coverage).
5. **Educate Policyholders and Insurance Producers**:

- Incentivize policyholder cyber hygiene by providing pricing policies, cybersecurity assessments, improvement recommendations, and general guidance.

6. **Obtain Cybersecurity Expertise**:
   - Ensure that your organization has the necessary expertise to navigate cyber risks effectively.
7. **Require Notice to Law Enforcement**:
   - Promptly report cyber incidents to relevant authorities.

These practices act as a catalyst for robust risk management and safeguarding economic interests in the financial domain. Their integration bolsters an organization's capacity to withstand cyber threats, ultimately fortifying its overall security posture.

Useful resources:

https://www.financialservicesperspectives.com/2021/03/new-cyber-insurance-risk-framework-provides-best-practices-for-the-insurance-industry/

https://www.ekransystem.com/en/blog/prepare-for-cyber-insurance

https://blog.rsisecurity.com/financial-cybersecurity-best-practices-for-financial-services-organizations/

7.2 Cyber Insurance During Vendor Selection

A critical factor during vendor selection revolves around the presence of cyber insurance. This insurance acts as a financial safeguard against potential losses stemming from cyber incidents or breaches impacting the vendor's offerings. Selecting vendors with cyber insurance coverage represents a sound strategic decision. Here's why:

- **Risk Mitigation**: Cyber insurance provides financial protection against data breaches, cyberattacks, and other security incidents. By choosing vendors with cyber insurance, you reduce the risk of financial losses due to cyber incidents.
- **Regulatory Compliance**: Some regulations and industry standards require organizations to work with vendors who have adequate cybersecurity measures, including cyber insurance. Ensuring your vendors comply with such requirements is essential.
  - **Trust and Resilience**: Vendors with cyber insurance demonstrate their commitment to cybersecurity excellence. Their coverage can help mitigate the impact of cyber incidents on your business operations.

If the organization decides not to prioritize cyber insurance during vendor selection, the following factors should be taken into consideration:

- **Risk Assessment**: Evaluate the specific risks associated with the vendor. If their services or products don't involve critical data or sensitive processes, cyber insurance may be less critical.
- **Alternative Risk Management**: Some organizations manage cyber risks through other means, such as robust contractual agreements, risk-sharing arrangements, or internal risk management practices.

Useful resources:

https://www.financialservicesperspectives.com/2021/03/new-cyber-insurance-risk-framework-provides-best-practices-for-the-insurance-industry/

https://agentsync.io/blog/technology/cybersecurity-and-insurance-exploring-the-nist-cybersecurity-framework

https://www.zeguro.com/blog/what-to-look-for-in-a-cyber-insurance-policy

7.3 Third-Party Risk Management (TPRM)

Effective third-party risk management (TPRM) safeguards your organization by proactively addressing risks associated with vendors. This involves thorough due diligence before onboarding, continuous monitoring of their security posture, and a well-defined incident response plan. By implementing a TPRM program, you can mitigate vulnerabilities introduced by third parties and ensure compliance with regulations like GDPR, which is especially critical in the banking and financial sector.

Conversely, neglecting TPRM exposes the organization to a cascade of potential issues, including cybersecurity breaches, operational disruptions, legal and regulatory non-compliance, and ultimately, reputational damage.

Useful resources:

https://www.upguard.com/blog/tprm-in-the-financial-sector

https://www.bluevoyant.com/knowledge-center/third-party-risk-management-tprm-a-complete-guide

https://www.nccgroup.com/us/newsroom/financial-stability-board-fsb-strengthens-its-guidance-on-third-party-risk-management-tprm/

https://www.upguard.com/blog/third-party-risk-management

7.4 Staying up-to-date to Monitor and Respond to Regulatory Updates

To effectively navigate the evolving environment of cybersecurity regulation within the banking and financial sector, organizations employ various strategies to monitor and respond to regulatory updates. This includes regular monitoring of regulatory changes, subscribing to regulatory news alerts for timely notifications, and actively participating in industry forums and conferences to stay informed and exchange best practices. By integrating these approaches, banking and financial institutions can adapt to regulatory changes swiftly and uphold their cybersecurity posture effectively.

- **Regular Monitoring of Regulatory Updates**: This involves actively tracking changes in regulations, guidelines, and policies related to cybersecurity. By staying informed, organizations can adapt their practices accordingly and ensure compliance with the latest requirements.
- **Subscription to Regulatory News Alerts**: Subscribing to relevant news alerts ensures that organizations receive timely notifications about regulatory developments. These alerts can cover updates from regulatory bodies, industry associations, and other relevant sources.
- **Participation in Industry Forums and Conferences**: Engaging in industry forums and conferences provides valuable insights into emerging trends, best practices, and regulatory updates. It allows organizations to learn from peers, experts, and regulators, fostering a proactive approach to cybersecurity.

Useful resources:

https://www.nortonrosefulbright.com/en/knowledge/publications/b8178be8/cybersecurity-not-just-an-it-issue-but-a-regulatory-one-too

https://www.ekransystem.com/en/blog/banking-and-financial-cyber-security-compliance

https://www.bis.org/fsi/publ/insights2.pdf