INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 15, Issue 4, (2025) E-ISSN: 2222-6990

The Role of Cybersecurity Governance in Enhancing the Sustainability of Jordanian Financial Institutions: Strategies and Trends

Khaw Khai Wah, Mohammad Rafiq Zureigat
School of Management, Universiti Sains Malaysia, Gelugor 11800, Penang, Malaysia
Email: khaiwah@usm.my
Corresponding Author Email: mohammadzreqat16@gmail.com

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v15-i4/25305 DOI:10.6007/IJARBSS/v15-i4/25305

Published Date: 21 April 2025

Abstract

Cybersecurity governance plays a pivotal role in enhancing the sustainability of financial institutions, especially with increasing reliance on technology. This study explores the role of cybersecurity governance in supporting the sustainability of Jordanian financial institutions, focusing on strategies to reduce cyber risks and ensure long-term stability. Reviewing current literature, the study emphasizes the importance of robust cybersecurity measures to protect institutions from evolving cyber threats. Findings highlight that effective information security management and proactive risk assessment are essential for operational continuity and the safeguarding of sensitive data. The study also examines Jordanian financial institutions' unique challenges and opportunities in adopting advanced cybersecurity practices, considering the country's regulatory environment and technological infrastructure. Results suggest that continuous advancements in cybersecurity frameworks and risk management strategies are critical to addressing emerging threats and supporting sustainable growth in the financial sector. The study offers practical recommendations for policymakers and practitioners in Jordan and similar regions, stressing the need for ongoing improvements in cybersecurity measures to ensure financial stability and enhance long-term resilience.

Keywords: Information Security Management and Cybersecurity, Cyber Risk Assessment and Management, Sustainability of Financial Institutions.

Introduction

Overview of Cybersecurity in Financial Institutions

Financial institutions are increasingly vulnerable to cyber threats due to their growing dependence on information technology (Soomro et al., 2016). Jordan, as a developing country, faces both opportunities and challenges in the realm of cybersecurity, a global issue that has gained significant attention in recent years (Amer et al., 2023; Abu Al-Haija, 2022; Al-Hanatla et al., 2024; Al-Jaloudi et al., 2024; Al-Khatib et al., 2025). This study explores how

effective cybersecurity governance can enhance the sustainability of financial institutions in Jordan, with an emphasis on strategies and innovations that mitigate cyber risks while ensuring long-term stability. In an era of rapid digital transformation, strong cybersecurity governance frameworks are crucial for protecting sensitive data, ensuring business continuity, and maintaining consumer trust in an increasingly complex digital environment (Cele & Kwenda, 2024; Nesakumar, 2022) .

The financial sector has witnessed a significant digital transformation in the 21st century, driven by advancements in information and communication technology. These have fundamentally reshaped how users access online services and products (Obasi, 2024; Soomro et al., 2016). However, this transformation has also brought about substantial security challenges, as the rise in cyber threats increasingly jeopardizes the confidentiality and integrity of financial data (Familoni & Shoetan, 2024; Dawodu et al., 2023; Despotović et al., 2023; Gulyas & Kiss, 2023). For Jordanian financial institutions, this presents both a challenge and an opportunity to align with global trends in digitalization while simultaneously addressing the associated cybersecurity risks (Bhargava, 2021; Al-Akkalik, 2025; Al-Khasawneh, 2023; Alsobeh et al., 2023).

While developed countries often have advanced cybersecurity infrastructures, developing nations like Jordan face significant challenges due to limited resources and relatively underdeveloped security practices (Familoni & Shoetan, 2024). Despite the growing interest in cybersecurity risk management, the specific elements that contribute to improving cybersecurity in such contexts remain poorly understood (Al-ma'aitah, 2022; Kumar et al., 2021). As technology has evolved, cybersecurity has become increasingly critical to the success or failure of financial institutions (Bulgurcu et al., 2010; De Arroyabe et al., 2023; Jeong, 2019; Karjalainen, 2019). In the past, cybersecurity concerns were minimal, particularly for standalone systems such as SCADA (Cherdantseva et al., 2016; Patel, 2005). Today, the cyber environment is viewed with equal importance as the physical world, with cybersecurity risks considered on par with real-world threats (Achuthan et al., 2025).

The performance of financial institutions globally has been significantly impacted by the increasing frequency and severity of cyberattacks (Hasan et al., 2021). Given that these attacks often target sensitive data such as personal records and client information, securing such data has become a critical priority for financial institutions (Familoni & Shoetan, 2024). As the financial sector plays a pivotal role in the global economy and handles highly sensitive data, its protection becomes paramount, especially as sectors across the economy increasingly rely on digital data management (Shulha et al., 2022; Familoni & Shoetan, 2024). With the ongoing acceleration of digitalization, the role of cybersecurity in achieving the Sustainable Development Goals (SDGs) is becoming more apparent. Cybersecurity is a continuous process that demands constant vigilance and adaptability (AL-Dosari & Fetais, 2023; Dawodu et al., 2023; Obasi, 2024; Odumesi & Sanusi, 2023). To effectively address emerging cyber threats such as malware and phishing, a comprehensive and adaptive risk assessment and mitigation approach is essential (Dawodu et al., 2023). Financial institutions are confronted with growing challenges in safeguarding their networks, especially as digital payments are expected to dominate by 2027 (Cele & Kwenda, 2024). Consequently, robust cybersecurity governance is critical not only for protecting digital assets but also for supporting the sustainability of financial institutions in the digital era.

Study Objectives: Enhancing Cybersecurity Governance for the Sustainability of Jordanian Financial Institutions

1. Strengthening Financial Institution Protection: To protect Jordanian financial institutions from cyberattacks and maintain their stability and continuity in the face of growing digital threats, the study intends to examine the function of cybersecurity governance.
2. Integrating Cybersecurity into Sustainability plans: To ensure safe and long-term growth for Jordanian financial institutions, the study aims to emphasize the significance of cyber risk management as a key element of sustainability plans.
3. Localized Insights for Sector Resilience: The study provides targeted insights into Jordan's cybersecurity challenges, offering practical recommendations to strengthen financial institutions and support national sustainable development goals.

Methodology

This literature review was meticulously designed to explore the governance of cybersecurity within Jordanian financial institutions. The process was organized to ensure a comprehensive and academically rigorous analysis, focusing on the evolving challenges associated with cybersecurity, their impact on the sustainability of financial institutions, and the integration of information security practices. This approach ensures a precise and reliable exploration of the subject, particularly in the context of rapid technological advancements (Siponen & Willison, 2009).

Data Sources

Data was gathered from reputable scientific databases such as Google Scholar, ScienceDirect, and IEEE Xplore, all of which are recognized for supporting high-quality academic research.

Search Strategy

Keywords such as "information security management," "cybersecurity," Cyber Risk Assessment and Management," and "sustainability of financial institutions" were utilized to identify relevant literature. Data collection began with an initial review of titles and abstracts, followed by a more in-depth examination of full texts to assess their relevance to the research objectives.

Inclusion and Exclusion Criteria for Relevant Literature

The selection of sources was guided by specific inclusion and exclusion criteria to ensure relevance and quality. The time frame for literature was set between 2015 and 2025 to capture the latest developments. The literature must explicitly focus on the intersection of information security management and cybersecurity, Cyber Risk Assessment and Management, and the sustainability of financial institutions, ensuring direct relevance to the study's objectives (Aturamu et al., 2021). Additionally, only English-language publications were included to ensure accessibility and accuracy in understanding.

Non-peer-reviewed articles, such as opinion pieces, editorials, and gray literature, were excluded to maintain academic rigor and source credibility (Akintuyi, 2024). Studies that did not focus on the study's main topics or lacked a clear methodology or supporting evidence were also excluded. Furthermore, publications in languages other than English were excluded to simplify the review process and ensure consistency in data analysis.

Data Analysis

The selected literature was analyzed using a content analysis approach. This process involved identifying common themes, patterns, challenges, and opportunities related to the role of cybersecurity governance, including information security management and cybersecurity and Cyber Risk Assessment and Management, in the sustainability of financial institutions. Key data were extracted, focusing on methodologies, findings, and conclusions relevant to the research objectives (Ayorinde et al., 2024). This approach ensures a comprehensive and accurate analysis of the latest trends in the field.

Literature Review

Recent studies have underscored the critical role of cybersecurity in ensuring the sustainability of financial institutions. Achuthan et al. (2025) and Sulich et al. (2021) highlighted the significant benefits that financial institutions can achieve by incorporating technologies such as machine learning and artificial intelligence into their cyber risk management strategies. These technologies empower institutions to better detect and respond to the increasing volume of cyber threats efficiently, thereby contributing to their long-term resilience and sustainability. In contrast, Cherdantseva et al. (2016) emphasized the importance of adopting systematic frameworks like NIST, which improve financial institutions' ability to identify and manage cyber risks effectively. These frameworks offer a flexible and structured approach, allowing institutions to address both evolving and emerging cyber threats.

Despite the advantages of these technologies and frameworks, financial institutions in Jordan still face significant challenges that hinder the enhancement of cybersecurity. Srouji et al. (2023) identified the lack of investment in cybersecurity infrastructure as a primary barrier to implementing effective security measures. Likewise, Omaiah et al. (2020) pointed out that the absence of modern technological tools restricts financial institutions' capacity to address growing cybersecurity challenges. Furthermore, the Central Bank of Jordan (2022) emphasized the difficulty in managing cyber risks due to a shortage of specialized human resources in this field.

In addition to technical challenges, security awareness remains a prominent issue for Jordanian financial institutions. Bani Khalid (2019) noted that the lack of cybersecurity awareness is one of the major obstacles preventing the effective implementation of cybersecurity strategies. Considering this, the adoption of advanced technologies like artificial intelligence is considered an effective solution to improve risk management and enhance the sustainability of financial institutions. This is particularly relevant in the context of Jordanian institutions, which face challenges such as limited access to modern technological tools and insufficient technical expertise. Kure et al. (2018) argued that these advanced technologies can help close the gap in cybersecurity risk management by providing scalable and intelligent solutions, which, in turn, increase the resilience of financial institutions against evolving cyber threats.

In response to these challenges, several studies have suggested comprehensive strategies to bolster cybersecurity within Jordanian financial institutions. AlDaajeh and Alrabaee (2024) proposed the development of comprehensive cybersecurity strategies to safeguard digital assets. Additionally, Srouji et al. (2023) underscored the importance of integrating green

innovation with cybersecurity to improve financial performance and enhance the sustainability of the financial sector. Similarly, Soomro et al. (2016) emphasized the necessity of adopting a holistic approach to information security management, allowing institutions to respond effectively to dynamic threats. While these studies offer valuable insights into the role of cybersecurity in strengthening the sustainability of financial institutions, the current literature is still limited to certain aspects, such as technology or legislation. There remains a notable gap in comprehensive frameworks that integrate various factors influencing the sustainability of financial institutions. Notably, there is a lack of studies that combine the legislative, technical, and cultural dimensions of cybersecurity, highlighting the need for an integrated framework to address these gaps.

Introduction to the Critical Importance of Cybersecurity in Financial Institutions

Cybersecurity has become an integral part of the strategic framework for financial institutions today. Research has shown that integrating cybersecurity measures into sustainability frameworks can enhance institutional performance and financial stability. Regulatory bodies also emphasize that incorporating sustainability into cybersecurity strategies not only improves financial outcomes but also fosters organizational resilience and supports the achievement of the Sustainable Development Goals (SDGs) (Khan et al., 2022; Von Solms & Van Niekerk, 2013; Xie et al., 2022). The growing cyber risks faced by financial institutions are undermining data security, threatening long-term viability, and potentially damaging the reputation and goals of organizations, especially amidst rapid technological advancements and increasing reliance on digital processes. As a result, strengthening cybersecurity has become a vital component of strategic planning for financial institutions, essential for protecting digital assets and ensuring business continuity (Gupta et al., 2023; Soomro et al., 2016).

This issue is particularly pressing in Jordan, where financial institutions face a dual challenge: embracing digital transformation while simultaneously dealing with the rising threat of cyberattacks. In this context, cybersecurity is critical for safeguarding financial assets, maintaining customer trust, and ensuring the overall stability and sustainability of the financial system (Alhanatleh et al., 2024; Al-Momani et al., 2024; Amer et al., 2023; Arabyat, 2023).

Effective cybersecurity management requires a balanced approach, involving investments in security measures while aligning with organizational goals in the face of escalating digital threats (Shao et al., 2020; Srinidhi, 2015). Research has pointed to the challenges faced by financial institutions in assessing the magnitude of cyberattacks and the resulting costs and data losses due to security breaches (De Arroyabe et al., 2023; Jalali et al., 2019). In this context, sustainable investments in cybersecurity can enhance an institution's reputation, attract socially responsible clients, and contribute to long-term profitability and sustainability (Samiun et al., 2024; Tariq et al., 2024). However, financial institutions often struggle to determine the optimal level of investment required to defend against increasingly sophisticated cyber threats (Shao et al., 2020). Studies have highlighted the difficulties faced by the financial sector in making such assessments, underscoring the need for comprehensive risk and cost evaluations (De Arroyabe et al., 2023; Shao et al., 2020; Srinidhi, 2015). Furthermore, many institutions fail to adequately invest in cybersecurity, leaving their digital assets vulnerable to cyberattacks (AL-Dosari & Fetais, 2023). This lack of understanding about

the importance of cybersecurity hinders institutions' ability to effectively counter emerging threats, reinforcing the need for a holistic strategic approach that integrates robust security measures at the organizational level (Familoni & Shoetan, 2024).

As such, financial institutions, regardless of their size, must recognize the cyber risks they face and adopt appropriate measures to ensure operational continuity and protect sensitive information (Kure et al., 2022). Cele and Kwenda (2024) project that global investments in cybersecurity will grow significantly, reaching $1.61 trillion by 2027, underscoring the increasing recognition of cybersecurity as a foundational element of sustainable business practices. In Jordan, the importance of cybersecurity in the financial sector has become even more evident as institutions struggle with increasingly sophisticated cyber threats. The sector's ability to effectively address these challenges through enhanced awareness, strong policy implementation, and adaptable strategies will play a critical role in securing the stability of Jordan's financial ecosystem and strengthening customer confidence in an era dominated by digital transformation.

Recent Trends in Enhancing Cybersecurity and Their Role in the Sustainability of Jordanian Financial Institutions

The Jordanian financial sector is undergoing a significant transformation driven by rapid advancements in digital technologies, which present new opportunities for economic growth. This section explores recent studies highlighting key trends that contribute to enhancing cybersecurity. A study by Al-Momani et al. (2024) emphasized the importance of adopting advanced security measures to fortify financial institutions' resilience, allowing them to counter cyber threats and, consequently, support their sustainability and competitiveness in the local market. Similarly, Alhanatleh et al. (2024) stressed the need to boost cybersecurity awareness among both users and institutions, thereby fostering trust in digital financial services and promoting greater stability within the financial sector. Moreover, Amer et al. (2023) focused on the role of advanced security technologies in mitigating cybercrime, asserting that such technologies effectively protect sensitive financial data while also enhancing the competitive advantage of banks. Additionally, Arabyat et al. (2023) proposed a strategic framework aimed at bolstering the resilience of Jordan's financial sector against cyber threats, highlighting the need to adopt modern technologies and strengthen collaboration between the public and private sectors in alignment with global best practices.

Increasing Reliance on Digital Technology and Cybersecurity Challenges in Jordanian Financial Institutions

The growing dependence on digital technology within Jordan's financial sector has introduced substantial security challenges, as the risks threatening the stability of financial institutions continue to intensify. Studies identify several major challenges, including insufficient cybersecurity awareness among employees and customers, as noted by Al-Kasassbeh et al. (2023). This gap in awareness increases financial institutions' vulnerability to cyberattacks and undermines the stability of the financial sector. Furthermore, Al-ma'aitah (2022) highlighted that outdated regulatory frameworks in Jordan are no longer adequate to address contemporary cyber threats, necessitating urgent updates to the legislation. Financial institutions also face difficulties in keeping pace with rapid technological advancements. Orelaja et al. (2024) noted that reliance on outdated technologies exacerbates security risks and limits institutions' capacity to adapt to the evolving digital environment. Moreover, Al-

Khasawneh (2023) pointed out the challenges associated with the adoption of advanced electronic accounting systems, which can protect financial data, but the inability of certain institutions to keep up with these developments jeopardizes their sustainability. Abulhaija et al. (2022) also observed a gap between theoretical knowledge of cybersecurity and its practical implementation within financial institutions, which complicates efforts to address growing threats. Finally, Al-Khatib et al. (2025) noted that cyberattacks erode trust among customers and business partners, negatively impacting revenues and threatening the stability of the financial sector.

Cybersecurity Governance: Frameworks and Dimensions

This section explores two fundamental elements of cybersecurity governance: information security management and cybersecurity, alongside the evaluation and management of cyber risks. These elements play a crucial role in strengthening the sustainability and resilience of financial institutions in Jordan by ensuring robust protection of digital infrastructure and effectively mitigating risks associated with cyber threats.

Information Security Management and Cybersecurity

Information security and cybersecurity management are foundational elements in safeguarding data and systems against the growing threats posed by cybercriminals. International standards, such as ISO 27001, emphasize the need for comprehensive frameworks to ensure the protection of information assets (Cele & Kwenda, 2024; Nesakumar, 2022). At its core, information security is guided by the principles of confidentiality, integrity, and availability (CIA Triad), which are achieved through rigorous risk management practices aimed at preventing unauthorized access, alteration, or destruction of data (AL-Dosari & Fetais, 2023). This approach extends beyond merely technological solutions, involving strategic and proactive measures to ensure business continuity and protect critical interests in an increasingly digital environment (Familoni & Shoetan, 2020; AlDaajeh & Alrabaee, 2024).

Cybersecurity, as defined by the International Telecommunication Union (ITU), refers to “a collection of tools, policies, security concepts, and safeguards designed to protect the cyber environment and organizational assets” (Familoni & Shoetan, 2020; Turk et al., 2022). It represents a more holistic and encompassing approach, safeguarding both informational and non-informational resources within an organization (Achuthan et al., 2025). Cybersecurity readiness reflects an organization's capacity to prevent and respond effectively to cyber incidents. A lack of readiness can undermine an organization’s ability to establish defenses, leaving digital assets vulnerable (Kure et al., 2018; Santorry, 2024; PRÁCE, 2021).

While closely related, information security and cybersecurity differ in their scope (Taherdoost, 2022; Venter et al., 2014; Solms & Solms, 2018). Information security covers all forms of information, whether physical or digital, while cybersecurity specifically focuses on the protection of digital assets such as networks, servers, and internet-connected devices (Brezavšček & Baggia, 2025). A common misconception is that information security is simply a subset of cybersecurity, which can lead organizations to overlook critical aspects of data protection and inadvertently expose themselves to greater risks (AlDaajeh & Alrabaee, 2024). Historically, information security management was heavily reliant on technological solutions, which proved insufficient in addressing the evolving nature of cyber threats. As these risks

became more sophisticated, the need for a more integrated approach, combining technical solutions with strategic management, became clear (Soomro et al., 2016; Singh et al., 2014). Additionally, cybersecurity is often confined to IT departments, which can result in fragmented communication and coordination across different organizational levels (Cherdantseva et al., 2016). To improve cybersecurity, best practices include the development of comprehensive security policies, fostering awareness among employees, providing continuous training, and ensuring that top management plays an active role in cybersecurity evaluations and decision-making processes (Doherty, 2009; Ernest Chang, 2007; Singh et al., 2014; Soomro et al., 2016).

In the financial sector, cybersecurity is essential for maintaining customer trust and ensuring the integrity of financial transactions. Crucial practices such as encryption, secure data storage, and robust access controls are necessary to protect sensitive financial information (Amer et al., 2023; Familoni & Shoetan, 2024; Achuthan et al., 2025). These measures not only enhance cyber resilience but also mitigate cybercrime, safeguarding critical infrastructure and the broader societal welfare (Al-ma'aitah, 2022; Gulyas & Kiss, 2023; Odebade, 2023).

Regulatory factors also significantly influence information security management. Larger financial institutions, which are more vulnerable to cyber threats, require more advanced security systems, while smaller organizations may face challenges due to the financial burden of implementing such measures (AL-Dosari & Fetais, 2023). To establish effective cybersecurity strategies, organizations need clear vision and robust governance, supported by comprehensive risk management frameworks and the sharing of threat intelligence (Kumar et al., 2020; Al-ma'aitah, 2022). Moreover, collaboration between the public and private sectors is essential to addressing common threats and ensuring a coordinated response to cybersecurity challenges (Sulich et al., 2021).

Cyber Risk Assessment and Management

Cybercrime has evolved into one of the most complex and multi-dimensional forms of criminal activity globally, characterized by an increasing variety of methods and sophisticated techniques (Stanikzai & Shah, 2021). As the cyber threat landscape continues to advance with the introduction of emerging technologies and increasingly complex attack methods, risk management practices need to adapt accordingly. Precise risk assessments are crucial for effectively addressing new and emerging threats (Kure et al., 2022). Managing internet-related risks is not a one-time task but an ongoing process that necessitates regular evaluations and updates to remain effective in a constantly evolving digital environment (Kavitha & Preetha, 2019). In this context, advanced technological solutions are pivotal in mitigating risks, particularly within the rapidly evolving financial sector (Santorry, 2024). Effective cyber risk management strategies are vital to safeguard the digital assets of financial institutions and minimize the potential disruptions caused by cyberattacks (Rondelez, 2018; Sumroo et al., 2016).

Cybersecurity risks can generally be categorized into three main areas: cybercrime, cyberattacks, and cyberterrorism (Almansoori et al., 2023). Broadly speaking, cyber risks refer to uncertain events resulting from system failures or malfunctions that negatively affect individuals, organizations, or the environment, thus hindering the achievement of strategic and operational goals (Kure et al., 2018). Key internet threats, such as malware, phishing,

unencrypted data, and insecure third-party services, can significantly impact online banking and financial transactions (Seal et al., 2024). These risks not only pose financial threats but also erode customer confidence in the global financial system (Fameloni & Shoetan, 2024). The field of cybersecurity has experienced significant development since its inception in the late 1960s, with terms like "computer security" (Madnick, 1978), "information security" (Bodin et al., 2008), "cyber risks management" (Carol Siegel et al., 2002), and "cybersecurity" (Von Solms & Van Niekerk, 2013) being used interchangeably. Despite this progress, confusion persists, making it challenging for organizations to address cyber risks cohesively (Schatz et al., 2017; Von Solms & Van Niekerk, 2013).

A proactive approach to cyber risk management enables organizations to identify vulnerabilities and strengthen the stability of their operations, particularly in the financial sector (Sumroo et al., 2016). Improving cyber risk management is not merely a technical issue but a strategic imperative, essential for ensuring business continuity amid growing cyber threats in the digital age. To maintain operational resilience, financial institutions must adopt effective cyber risk management strategies that focus on threat identification, impact assessment, and the implementation of preventive measures (Al-ma'aitah, 2022; Mandritsa et al., 2018; Espinoza et al., 2020; Samiun et al., 2024).

An effective cyber risk management process entails evaluating various factors, including the severity and significance of the risks an organization faces (Kure et al., 2022). This involves identifying potential threats, assessing their likelihood, and implementing controls to protect digital assets from breaches and cyberattacks (AL-Dosari & Fetais, 2023; Tam et al., 2021). Advanced techniques, such as risk mitigation and risk transfer technologies, have been developed to reduce residual risks to acceptable levels, thus enhancing the overall effectiveness of risk management efforts (Kure et al., 2022; Carol Siegel et al., 2002; Marotta & McShane, 2018; McShane et al., 2021).

As operational risks, including fraud, system failures, and human errors, continue to increase, financial institutions face greater vulnerability to sophisticated cyberattacks exploiting these weaknesses (Fameloni & Shoetan, 2024). For instance, the 2019 Cybersecurity Breaches Survey (CSBS) found that over 33% of managers do not receive regular cybersecurity updates, highlighting a lack of coordination and security awareness among senior leadership. Only 21% of top executives receive these updates on a daily or weekly basis, which heightens the exposure to advanced cyber threats (De Arroyabe et al., 2023).

The World Economic Forum (2024) predicts that the global cost of cybercrime will reach $10.5 trillion by 2025, growing at an annual rate of 15%. In the financial sector, cyberattacks could result in losses ranging from $270 billion to $350 billion annually if their frequency continues to increase (Achuthan et al., 2025). In Jordan, cyberattacks have surged dramatically, with a notable 80% rise in cybersecurity incidents in 2023 compared to 2022, totaling 2,455 incidents in 2023 versus 1,362 in 2022 (National Cybersecurity Center, 2023). In the first quarter of 2024, the number of attacks rose by 124% compared to the last quarter of 2023 (Al-Mbaideen, 2024).

Despite ongoing efforts to enhance cybersecurity, the financial costs continue to escalate, emphasizing the critical need for strategic risk management within financial institutions

(McShane et al., 2021; Deniran et al., 2024). A robust cyber risk management strategy aligns organizational goals with risk management practices, enhancing protection against digital threats (Al-ma'aitah, 2022a; Fameloni & Shoetan, 2024). While financial institutions face significant challenges in implementing such strategies, leveraging technological advancements can improve their ability to predict, monitor, and respond to risks more effectively (Santorry, 2024).

Sustainability of Financial Institutions: Economic, Social, and Environmental Dimensions

The concept of sustainability in financial institutions has gained significant importance in recent years, expanding to include economic, social, and environmental dimensions in addition to traditional goals such as profitability and operational survival (Jan et al., 2021; Shad, 2020). Historically, financial institutions have primarily focused on financial objectives, like profits and market stability. However, contemporary challenges, such as economic instability and increasing social awareness, have prompted a broader perspective. These challenges have driven institutions to adopt strategies that ensure long-term sustainability, improve competitive advantage, and enhance customer satisfaction (Ali et al., 2021).

Sustainable development, as articulated by the Brundtland Report (1987), refers to the ability to meet present needs without compromising the ability of future generations to meet their own needs (Ali et al., 2021; Kuo et al., 2023). In the financial sector, achieving sustainability requires balancing economic, social, and environmental goals. Financial institutions are instrumental in driving economic growth, fostering innovation, and generating employment, particularly in developing economies (Kuo et al., 2023).

In Jordan, the financial sector has made substantial progress toward sustainability, with a notable contribution from the rapid expansion of the information and communication technology (ICT) sector, which has been growing at an annual rate of 25% (Srouji et al., 2023). This growth is pivotal for achieving key social and economic development goals, including the enhancement of digital services and the promotion of financial inclusion. Jordan has set an ambitious goal of transitioning to a fully digital economy by 2025, as outlined by the United Nations Conference on Trade and Development (UNCTAD, 2022).

Jordan's commitment to sustainability is further reflected in the advancements within its financial sector. For instance, the inclusion of the Amman Stock Exchange in the Sustainable Stock Exchanges Initiative in early 2017 marks a significant step in integrating environmental, social, and governance (ESG) frameworks into financial practices (Tawfik et al., 2021; Bani Khalid, 2019). This integration not only improves transparency but also directs investments toward sustainable projects, thereby supporting the country's national development objectives.

The concept of "social sustainability" emphasizes the need to align economic, social, and environmental goals to achieve long-term sustainability. Within this framework, the financial sector plays a crucial role in achieving these objectives (Jan et al., 2021; Morioka & de Carvalho, 2016). For investors, sustainability is increasingly associated with companies that demonstrate strong performance in environmental stewardship, social responsibility, and corporate governance (ESG). This approach reinforces the potential of capitalism to foster lasting sustainability (Kuo et al., 2023).

Despite the growing emphasis on sustainability, studies reveal that environmental and social disclosures in the financial sector remain insufficient (Day, 2009; Kuo et al., 2023). Moreover, the sector's performance in social responsibility is often considered inadequate (Kuo et al., 2023; Weber, 2014). These challenges highlight the difficulties that financial institutions face in fully aligning with the United Nations Sustainable Development Goals (SDGs). Achieving these goals requires robust collaboration between the public and private sectors (Jan et al., 2021; Naciti, 2019). In 2015, the United Nations called on governments to implement national strategies aimed at achieving these goals (Kuo et al., 2023). This underscores the need for financial institutions to adopt a more integrated approach to sustainability, balancing economic, social, and environmental objectives to ensure both short-term success and long-term resilience.

Cybersecurity Governance and Its Role in the Sustainability of Financial Institutions

The intersection of cybersecurity governance, environmental protection, and sustainable development is vital for achieving a sustainable future. As digital infrastructure and data play increasingly central roles in both societal and business operations, safeguarding these systems is critical for maintaining the integrity of efforts aimed at achieving the Sustainable Development Goals (SDGs) (Chukwurah et al., 2024; Ige et al., 2024; Obasi, 2024). In this context, cybersecurity governance encompassing information security management, cybersecurity, and cyber risk assessment becomes a crucial factor in enhancing the sustainability of financial institutions, especially in the face of rising cyber threats (Savash & Karatas, 2022; Solekh et al., 2021; Chukwurah et al., 2024).

Cybersecurity has evolved from a technical concern to a strategic and essential component of modern financial institutions. Its role extends beyond addressing technical risks to ensuring overall business sustainability and resilience against emerging cyber threats (De Arroyabe et al., 2023; Obasi, 2024). Cybersecurity governance is foundational in fostering sustainability within financial institutions by securing critical systems and data (Savaş & Karatas, 2022; Morales-Sáenz et al., 2024; Obasi, 2024).

The connection between cybersecurity and sustainable development is also evident through the concept of "green cybersecurity." This concept focuses on minimizing the environmental impact of digital systems while simultaneously protecting them from growing cyber threats (Achuthan et al., 2025; Abrahams, 2024; Adewusi et al., 2024; Obasi, 2024; Reis, 2024). Green cybersecurity is instrumental in achieving the SDGs by securing digital platforms that underpin e-government services and broader sustainability initiatives (Obasi, 2024; Udoufimhe, 2023). It also ensures the safety of data and digital systems that support green development projects, thereby safeguarding business continuity and reducing operational risks associated with cyber threats (Obasi, 2024; Suku et al., 2023).

As the financial sector becomes more reliant on technology, integrating cybersecurity practices into the SDGs has become crucial. This integration aims to create secure digital environments that promote environmental, social, and economic sustainability (Obasi, 2024). However, the advent of emerging technologies, such as complex algorithms and digital currencies, introduces the potential for increased carbon emissions, posing additional challenges to the sustainability of digital systems (Akana, 2023; Achuthan et al., 2025).

Cybersecurity is also paramount for maintaining trust between financial institutions and their customers. Ilogi et al. (2016) observed that any breach in information security could disrupt operations significantly, leading to substantial financial losses and a loss of customer confidence. As a result, cybersecurity has become a cornerstone for ensuring the long-term sustainability of financial institutions in the digital era (Achuthan et al., 2025; Obasi, 2024).

Risk management strategies are equally important in ensuring sustainability. These strategies enable financial institutions to identify potential threats, assess their impacts, and protect against disruptions that could jeopardize business continuity (Samiun et al., 2024). Mutamimah et al. (2022) highlight the need to evaluate the sustainability of smaller financial institutions from a risk management perspective, an area that remains underexplored.

Jordan has made substantial progress in its digital transformation, with a strong emphasis on enhancing cybersecurity. This includes the introduction of the Cybersecurity Law in 2019 and the establishment of the National Cybersecurity Center in 2021, which plays a central role in monitoring and responding to cyberattacks. Additionally, the National Cybersecurity Council, established in 2021, has been instrumental in promoting cross-sector collaboration and developing effective national cybersecurity policies (National Cybersecurity Center, 2023).

In 2024, the Jordanian government approved the National Plan to Combat Cyber Threats, which aims to ensure business continuity and protect individuals and data from the rising risks associated with cyberattacks (Jordan News Agency, Petra, 2024). Financial institutions, including banks, are now being encouraged to provide adequate insurance coverage to mitigate financial losses resulting from the growing frequency of cyberattacks (Al-Akaleek, 2024).

Strategies for Enhancing Cybersecurity in Jordanian Financial Institutions

To achieve sustainable cybersecurity in Jordanian financial institutions, comprehensive strategies must be adopted. A study by Al-Akkalik (2025) highlighted the need to update legislative frameworks to protect data in line with rapid digital developments. Institutions should also invest in advanced security technologies such as artificial intelligence and machine learning to strengthen defenses against cyberattacks. Alsobeh et al. (2023) recommended enhancing security awareness through intensive training programs for employees and customers to reduce insecure behaviors. The Central Bank of Jordan's report (2022) emphasized the importance of strengthening collaboration between the public and private sectors to share expertise and best practices in cybersecurity. Finally, financial institutions should adopt an integrated strategic framework for managing cybersecurity risks, including periodic risk assessments and effective incident response plans.

Recommendations

To ensure a secure and sustainable digital environment, financial institutions in Jordan should:

1. Regularly update protection systems and adopt modern technologies to keep up with evolving cyber threats.
2. Increase employee and customer awareness through continuous training and awareness programs to promote secure digital practices.
3. Adopt international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework to enhance global competitiveness and align with best practices.

4. Strengthen collaboration between the public and private sectors to share knowledge and resources in addressing cyber threats.
5. Develop and regularly test incident response plans to minimize the impact of cyberattacks and ensure business continuity.
6. Explore advanced technologies such as artificial intelligence and blockchain to strengthen cybersecurity and protect digital infrastructure.

Conclusion

Cybersecurity governance plays a pivotal role in enhancing the sustainability of Jordanian financial institutions by reducing cyber risks and ensuring long-term stability. This sustainability relies on practical information security management, proactive risk assessment, and the ability to adapt to evolving cyber threats. The Jordanian financial sector can achieve sustainable growth and maintain customer trust amid rapid digital transformation by fostering collaboration between the public and private sectors, adopting international standards, and continuously improving security measures. This study emphasizes the importance of developing robust security strategies to support the resilience and sustainability of financial institutions in Jordan and similar regions.

References

Abrahams, T. O. (2024). A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection. *Omputer Science & IT Research Journal*, *5*(1), 1–25.

Achuthan, K., Sankaran, S., Roy, S., & Raman, R. (2025). Integrating sustainability into cybersecurity: insights from machine learning based topic modeling. *Discover Sustainability*, *6*(1), 44. https://doi.org/10.1007/s43621-024-00754-w

Adewusi, A. O., Okoli, U. I., Adaga, E., Olorunsogo, T., Asuzu, O. F., &, & Daraojimba, D. O. (2024). BUSINESS INTELLIGENCE IN THE ERA OF BIG DATA: A REVIEW OF ANALYTICAL TOOLS AND COMPETITIVE ADVANTAGE. *Computer Science & IT Research Journal*, *5*(2), 415–431. https://doi.org/10.51594/csitrj.v5i2.791

Akintuyi, O. B. (2024). AI in agriculture: A comparative review of developments in the USA and Africa. *Research Journal of Science and Engineering*, *10*(02), 060–070.

Al-Akaleek, Dr. H. (2024). Strengthening financial institutions (Jordanian banks) against cyber threats using advanced security strategies. *Khaberni*. Retrieved from https://www.khaberni.com/news/تحصين-المؤسسات-المالية-البنوك-الاردنية-ضد-التهديدات-الس-635782

Al-Akkalik, H. (2025). Legal frameworks for cybersecurity in Jordan. *Al-Ghad Newspaper. Retrieved Fromhttps://Alghad.Com/1909699*, 1.

AlDaajeh, S., & Alrabaee, S. (2024). Strategic cybersecurity. *Computers and Security*, *141*. https://doi.org/10.1016/j.cose.2024.103845

AL-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics (Switzerland)*, *12*(17). https://doi.org/10.3390/electronics12173629

Alhanatleh, H., Khaddam, A., Abudabaseh, F., Alghizzawi, M., & Alzghoul, A. (2024). Enhancing the public value of mobile fintech services through cybersecurity awareness antecedents: A novel framework in Jordan. *Investment Management and Financial Innovations*, *21*(1), 417–430. https://doi.org/10.21511/imfi.21(1).2024.32

Ali, B. J. A., Salem, M., Umm, O., & Quwain, A. (2021). *ACCOUNTING INFORMATION SYSTEM AND FINANCIAL SUSTAINABILITY OF COMMERCIAL AND ISLAMIC BANKS: A REVIEW OF THE LITERATURE*. https://www.researchgate.net/publication/352020143

Aljaloudi, O., Dacre, N., & Al-Mhdawi, M. K. S. (2024). *Decoding the Nexus Between Credit Risk Challenges and Banks Performance: Perspectives from Commercial Banks in Jordan*.

Al-Kasassbeh, F. Y., Ghazleh, A. M. A., Kareem, M. J. M., & breizat, M. O. (2023). International and National Efforts to Protect Cyber Security: Jordan Case Study. *International Journal of Cyber Criminology*, *17*(2), 350–363. https://doi.org/10.5281/zenodo.4766720

Al-Khasawneh, R. O. (2023). Importance of Electronic Accounting Information Systems in Improving Financial Information Security in Jordanian Electronic Payment and Money Transfer Companies. *International Journal of Professional Business Review*, *8*(7), e02777. https://doi.org/10.26668/businessreview/2023.v8i7.2777

Al-Khatib, S. F., Ibrahim, Y. Y., & Alnadi, M. (2025). Cybersecurity Practices and Supply Chain Performance: The Case of Jordanian Banks. *Administrative Sciences*, *15*(1). https://doi.org/10.3390/admsci15010001

Al-ma'aitah, M. A. (2022). Investigating the drivers of cybersecurity enhancement in public organizations: The case of Jordan. *Electronic Journal of Information Systems in Developing Countries*, *88*(5). https://doi.org/10.1002/isd2.12223

Almaiah, M. A., Al-Khasawneh, A., & Althunibat, A. (2020). Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic. *Education and Information Technologies*, *25*(6), 5261–5280. https://doi.org/10.1007/s10639-020-10219-y

Al-Mamlaka TV. (2024). Cybersecurity: We dealt with 2,455 cybersecurity incidents last year. *Https://Bit.Ly/3x2yZ3B*, 1.

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. In *Applied Sciences (Switzerland)* (Vol. 13, Issue 9). MDPI. https://doi.org/10.3390/app13095700

Al-Mbaideen, I. (2024). Cyber threats plan... Does it protect the data of organizations and individuals? Alghad. Retrieved from https://alghad.com/Section-181/-اقتصاد/خطة-مواجهة-التهديدات-السيبرانية-هل-تحمي-بيانات-المؤسسات-والأفراد-1685767

Al-Momani, A. M., Sarram, M., Zighan, S. M., Al-Majali, R. T., Al-shanableh, N., Saatchi, S. G., Shatnawi, T. M., Alajarmeh, N. S., Al-Hawary, S. I. S., & Mohammad, A. A. S. (2024). The Influence of Cybersecurity Leadership on the Resilience of Jordanian Businesses: A Study on the Role of Cybersecurity Measures in Entrepreneurial Success. In *Studies in Computational Intelligence* (Vol. 1152, pp. 1–15). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-57242-5_1

Alsobeh, A. M. R., Alazzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online Journal of Communication and Media Technologies*, *13*(2). https://doi.org/10.30935/ojcmt/12942

Amer, T. B., Ibrahim, M., & Al-Omar, A. (2023a). The Impact of Cyber Security on Preventing and Mitigating Electronic Crimes in the Jordanian Banking Sector. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 14, Issue 8). www.ijacsa.thesai.org

Arabyat, Y. A. (2023). Overview of cybersecurity trends in Jordan's financial sector. *In International Conference of Reliable Information and Communication Technology*, 285–292.

Aturamu, O. A., Thompson, O. A., &, & Akintuyi, B. O. (2021). FORECASTING THE EFFECT OF CLIMATE VARIABILITY ON YAM YIELD IN RAIN FOREST AND GUINEA SAVANNAH AGRO-ECOLOGICAL ZONE OF NIGERIA. FORECASTING THE EFFECT OF CLIMATE VARIABILITY ON YAM YIELD IN RAINFOREST AND GUINEA SAVANNAH AGRO-ECOLOGICAL ZONE OF NIGERIA. *Original Research Article Journal of Global Agriculture and Ecology*, *11*(4), 1–12. https://www.researchgate.net/publication/354282449

Ayorinde, O. B., Etukudoh, E. A., Nwokediegwu, Z. Q. S., Ibekwe, K. I., Umoh, A. A., Hamdan, A., & Igbinenikaro, O. P. (2024). Renewable energy projects in Africa: A review of climate finance strategies. *International Journal of Science and Research Archive*, *11*(1), 923–932.

BAKALÁŘSKÁ PRÁCE. (2021). *3830 | Sanjiv Kumar An Analysis Of The Problems And Issues With Cyber Security An Analysis Of The Problems And Issues With Cyber Security*. *20*(4), 3830–3836. https://doi.org/10.17051/ilkonline.2021.04.419

Bani-Khalid, T. (2019). Examining the quantity and quality of online sustainability disclosure within the Jordanian industrial sector: A test of GRI guidelines. *Problems and Perspectives in Management*, *17*(4), 141–152. https://doi.org/10.21511/ppm.17(4).2019.12

Bhargava, R. (2021). Cyber Crime And Cyber Security In Madhya Pradesh. *NJESR*, 1–9. https://doi.org/10.53571/NJESR

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM*, *51*(4), 64–68. https://doi.org/10.1145/1330311.1330325

Brezavšček, A., & Baggia, A. (2025). Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review. In *Systems* (Vol. 13, Issue 1). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/systems13010052

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning*, *48*(4), 265–276. https://doi.org/10.1016/j.lrp.2014.07.005

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). *SPECIAL ISSUE INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS 1*. http://www.misq.org

Carol Siegel, B. A., Sagalow, T. R., & Serritella, P. (2002). *Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security*.

Cele, N. N., & Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. In *Journal of Financial Crime*. Emerald Publishing. https://doi.org/10.1108/JFC-10-2023-0263

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. In *Computers and Security* (Vol. 56, pp. 1–27). Elsevier Ltd. https://doi.org/10.1016/j.cose.2015.09.009

Chukwurah, E. G., Okeke, C. D., &, & Ekechi, C. C. (2024). Innovation green technology in the age of cybersecurity: Balancing sustainability goals with security concerns. *Computer Science & IT Research Journal*, *5*(5), 1048–1075. https://doi.org/10.51594/csitrj.v5i5.1115

Dawodu, S. O., Akindote, O. J. , Adegbite, A. O., & Ewuga, S. K. (2023). CYBERSECURITY RISK ASSESSMENT IN BANKING: METHODOLOGIES AND BEST PRACTICES. *Computer Science & IT Research Journal*, *4*(3), 220–243. https://doi.org/10.51594/csitrj.v659

Day, R., & W. T. (2009). CSR reporting and the UK financial services sector. *Ournal of Applied Accounting Research, 10*(3), 159–175.

De Arroyabe, I. F., Arranz, C. F., Arroyabe, M. F., & de Arroyabe, J. C. F. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers and Security*, *124*. https://doi.org/10.1016/j.cose.2022.102954

deniran, I. A., Abhulimen, A. O. , Obiki-Osafiele, A. N., Osundare, O. S., Agu, E. E., &, & Efunniyi, C. P. (2024). Strategic risk management in financial institutions: Ensuring robust regulatory compliance. *Finance & Accounting Research Journal*, *6*(8), 1582–1596. https://doi.org/10.51594/farj.v6i8.1508

Despotović, A., Parmaković, A., &, & Miljković, M. (2023). Cybercrime and cyber security in fintech. *In Digital Transformation of the Financial Industry: Approaches and Applications* , 255–272.

Doherty, N. F. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, *29*(6), 449–457.

Elogie, A., Joy Ikenwe, I., Magnus Igbinovia, O., & Ann Elogie, A. (2016). Information Security in the Digital Age: The Case of Developing Countries. In *Chinese Librarianship: an International Electronic Journal*.

Ernest Chang, S. , & L. C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438–458.

Espinoza, A. M. R., Nina, E. D. M., &, & Dávila, G. D. (2020). *Estrategias financieras sostenibles aplicadas ante situaciones de riesgo empresarial: un análisis bibliográfico Sustainable financial strategies applied to business risk situations: a literature review*.

Familoni, B. T., &, & Shoetan, P. O. (2020). Information and cyber security maturity models: a systematic literature review. In *Information and Computer Security* (Vol. 28, Issue 4, pp. 627–644). Emerald Group Holdings Ltd. https://doi.org/10.1108/ICS-03-2019-0039

Familoni, B. T., &, & Shoetan, P. O. (2024). CYBERSECURITY IN THE FINANCIAL SECTOR: A COMPARATIVE ANALYSIS OF THE USA AND NIGERIA. *Computer Science & IT Research Journal*, *5*(4), 850–877. https://doi.org/10.51594/csitrj.v5i4.1046

Gulyas, O., & Kiss, G. (2023). Impact of cyber-Attacks on the financial institutions. *Procedia Computer Science*, *219*, 84–90. https://doi.org/10.1016/j.procs.2023.01.267

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*. https://doi.org/10.1016/j.jisa.2020.102726

Ige, A. B., Kupa, E., & Ilori, O. (2024). Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future. *GSC Advanced Research and Reviews*, *19*(3), 344–360. https://doi.org/10.30574/gscarr.2024.19.3.0236

Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *Journal of Strategic Information Systems*, *28*(1), 66–82. https://doi.org/10.1016/j.jsis.2018.09.003

Jan, A. A., Lai, F. W., & Tahir, M. (2021). Developing an Islamic Corporate

Governance framework to examine sustainability performance in Islamic Banks and Financial Institutions. *Journal of Cleaner Production*, *315*. https://doi.org/10.1016/j.jclepro.2021.128099

Jordan News Agency (Petra). (2024). Jordan enhances international cooperation in cybersecurity. *Https://Www.Pm.Gov.Jo.*, 1–1.

Karjalainen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Information Systems Research*, *30*(2), 687–704.

Kavitha, V., & Preetha, S. (2019). CYBER SECURITY ISSUES AND CHALLENGES - A REVIEW. *A Monthly Journal of Computer Science and Information Technology*, *8*(11), 1–6.

Khan, A. W., Zaib, S., Khan, F., Tarimer, I., Seo, J. T., & Shin, J. (2022). Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach. In *IEEE Access* (Vol. 10, pp. 65044–65054). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2022.3179822

Kumar, P., Kumar, A. A., Sahayakingsly, C., & Udayakumar, A. (2021). Analysis of intrusion detection in cyber attacks using DEEP learning neural networks. *Peer-to-Peer Networking and Applications*, *14*(4), 2565–2584. https://doi.org/10.1007/s12083-020-00999-y

Kuo, Y. C., Huang, Y. H., Sun, L., Small, G., & Lin, S. J. (2023). Identifying key factors of sustainability practice in financial institutions based on decision-making trial and evaluation laboratory method. *Asian Review of Accounting*, *31*(5), 661–679. https://doi.org/10.1108/ARA-07-2022-0164

Kure, H. I., Islam, S., & Mouratidis, H. (2022). *An Integrated Cyber Security Risk Management Framework and Risk Predication for the Critical Infrastructure Protection*.

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences (Switzerland)*, *8*(6). https://doi.org/10.3390/app8060898

Madnick, S. E. (1978). Management policies and procedures needed for effective computer security. *Sloan Management Review (Pre-1986)*, *20*(1:61).

Marotta, A., & McShane, M. (2018). Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach. *Risk Management and Insurance Review*, *21*(3), 435–452. https://doi.org/10.1111/rmir.12109

McShane, M., Eling, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93–125. https://doi.org/10.1111/rmir.12169

Morioka, S. N., & de Carvalho, M. M. (2016). A systematic literature review towards a conceptual framework for integrating sustainability performance into business. *Ournal of Cleaner Production*, *136*, 134–146.

Mutamimah, M., Zaenudin, Z., & Bin Mislan Cokrohadisumarto, W. (2022). Risk management practices of Islamic microfinance institutions to improve their financial performance and sustainability: a study on Baitut Tamwil Muhammadiyah, Indonesia. *Qualitative Research in Financial Markets*, *14*(5), 679–696. https://doi.org/10.1108/QRFM-06-2021-0099

Naciti, V. (2019). *ACCEPTED MANUSCRIPT Corporate governance and board of directors: the effect of a board composition on firm sustainability performance*.

National Cyber Security Center. (2023). *The Reality of Cybersecurity in Jordan 2023*.

Nesakumar, D. (2022). Smart ATM card for multiple bank accounts. *In 2022 International Interdisciplinary Humanitarian Conference for Sustainability*, 1228–1232.

Obasi, S. C. (2024). Cybersecurity's role in environmental protection and sustainable development: Bridging technology and sustainability goals. *Computer Science & IT Research Journal, 5*(5), 1145–1177.

Odebade, A. T. (2023). *A Comparative Study of National Cyber Security Strategies of ten nations*.

Odumesi, J. O., & Sanusi, B. S. (2023). Achieving Sustainable Development Goals from a Cybersecurity Perspective. *Advances in Multidisciplinary and Scientific Research Journal Publication*, *2*(1), 1–10. https://doi.org/10.22624/aims/csean-smart2023p3

Patel, S. (2005). Supervisory control and data acquisition remote terminal unit testbed. *Intelligent Systems Research Laboratory Technical Report TR-ISRL-05-01, Department of Computer Engineering and Computer Science. Louisville, Kentucky: University of Louisville*, 24–26.

Reis, O. (2024). Privacy law challenges in the digital age: a global review of legislation and enforcement. *International Journal of Applied Research in Social Sciences*, *6*(1), 73–88.

Rondelez, R. (2018). Governing cyber security through networks: An analysis of cyber security coordination in Belgium. *International Journal of Cyber Criminology*, *12*(1), 300–315. https://doi.org/10.5281/zenodo.1467929

Samiun, A. A. , Sudarmanto, E., Gilaa, T., Majid, J., & Purwanto, P. (2024). The Effect of Financial Planning, Sustainable Investment, and Risk Management on Business Sustainability in the SME Sector. *Sciences Du Nord Economics and Business*, *1*(02), 100–108. https://doi.org/10.58812/2f7qkk43

Santorry, S. (2024). *Evaluating the Impact of Technological Innovations on Operational Risk Management in Financial Institutions*. https://thejoas.com/index.php/

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. International Cybersecurity Law Review, 3(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2017.1476

Shad, M. K. (2020). The efficacy of sustainability reporting towards cost of debt and equity reduction. *Environmental Science and Pollution Research, 27*, 22511–22522.

Shao, X., Siponen, M., & Liu, F. (2020). Shall we follow? Impact of reputation concern on information security managers' investment decisions. *Computers and Security*, *97*. https://doi.org/10.1016/j.cose.2020.101961

Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking Information Resource Cybersecurity System Modeling. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(2). https://doi.org/10.3390/joitmc8020080

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management." *Journal of Enterprise Information Management*, *27*(5), 644–667. https://doi.org/10.1108/JEIM-07-2013-0052

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information and Management*, *46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Srinidhi, B. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems*, *75*, 49–62.

Srouji, A. F., Hamdallah, M. E., Al-Hamadeen, R., Al-Okaily, M., & Elamer, A. A. (2023). The impact of green innovation on sustainability and financial performance: Evidence from the Jordanian financial sector. *Business Strategy and Development*, *6*(4), 1037–1052. https://doi.org/10.1002/bsd2.296

Stanikzai, A. Q., & Shah, M. A. (2021). Evaluation of Cyber Security Threats in Banking Systems. *2021 IEEE Symposium Series on Computational Intelligence, SSCI 2021 - Proceedings*. https://doi.org/10.1109/SSCI50451.2021.9659862

Suku, P. G., Ugwoha, E., Orikpete, O. F., & Ewim, D. R. E. (2023). Assessment of respiratory and reproductive impacts of artisanal refinery activities on male Albino Wistar rats: implications for environmental health. *Bulletin of the National Research Centre*, *47*(1). https://doi.org/10.1186/s42269-023-01121-x

Sulich, A., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and sustainable development. *Procedia Computer Science*, *192*, 20–28. https://doi.org/10.1016/j.procs.2021.08.003

Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, *215*, 483–487. https://doi.org/10.1016/j.procs.2022.12.050

Tam, T., Rao, A., & Hall, J. (2021). *The Good, The Bad and The Missing: A Narrative Review of Cyber-security Implications for Australian Small Businesses*. https://doi.org/10.1016/j.cose.2021.102385

Tariq, E., Akour, I., Al-Shanableh, N., Alquqa, E. K., Alzboun, N., Al-Hawary, S. I. S., & Altruize, M. T. (2024). How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. *International Journal of Data and Network Science*, *8*(1), 69–76. https://doi.org/10.5267/j.ijdns.2023.10.016

Tawfik, O. I., Kamar, S. H., & Bilal, Z. O. (2021). The Effect of Sustainable Dimensions on the Financial Performance of Commercial Banks: A Comparative Study in Emerging Markets. *Journal of Asian Finance, Economics and Business*, *8*(3), 1121–1133. https://doi.org/10.13106/jafeb.2021.vol8.no3.1121

Turk, Ž., García de Soto, B., Mantha, B. R. K., Maciel, A., & Georgescu, A. (2022). A systemic framework for addressing cybersecurity in construction. *Automation in Construction*, *133*. https://doi.org/10.1016/j.autcon.2021.103988

Uduafemhe, M. E. (2023). *Adapting to the New Normal: Equipping Career and Technical Education Graduates with Essential Digital Skills for Remote Employment*. https://www.researchgate.net/publication/375599146

United Nations Conference on Trade and Development (UNCTAD). (2022). Jordan: Assessment of readiness for e-commerce. *Https://Unctad.Org/System/Files/Official-Document/Dtlstict2021d6_ar.Pdf*, *UNCTAD/DTL/STICT, Ed*, 3–122.

Venter, H. S., Loock, M., Coetzee, M., & Eloff, M. M. (2014). *From Information Security to Cyber Security Cultures: In 2014 Information Security for South Africa (pp. 1-7). Vol. IEEE*.

Von Solms, B., &, & Von Solms, R. (2018). Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where? *Information & Computer Security*, *26*(1), 2–9.

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

Weber, O. (2014). Corporate social responsibility of the financial sector–strengths, weaknesses and the impact on sustainable development. *Sustainable Development, 22*(5), 321–335.

Xie, Z., Liu, X., Najam, H., Fu, Q., Abbas, J., Comite, U., Cismas, L. M., & Miculescu, A. (2022). Achieving Financial Sustainability through Revenue Diversification: A Green Pathway for Financial Institutions in Asia. *Sustainability (Switzerland)*, *14*(6). https://doi.org/10.3390/su14063512