CyberFusion Protocols: Strategic Integration of Enterprise Risk Management, ISO 27001, and Mobile Forensics for Advanced Digital Security in the Modern Business Ecosystem

Abstract

This research paper explores the integration of Enterprise Risk Management (ERM), the ISO 27001 standard, and mobile forensics methodologies as a comprehensive framework for enhancing digital security measures within modern business ecosystems. Employing a quantitative research design, this paper utilized a survey methodology, gathering data from 372 professionals across various sectors including risk management, IT/security, and forensic analysis. The analysis was conducted using Partial Least Squares Structural Equation Modeling (PLS-SEM) to test the research hypotheses and assess the impact of the integrated approach on organizational digital security capabilities. The findings reveal a significant positive effect of integrating ERM, ISO 27001, and mobile forensics on an organization's ability to manage digital risks effectively. Specifically, the integrated approach was found to enhance strategic digital security management, improve the identification, assessment, and mitigation of digital risks, strengthen information security management practices, and elevate the effectiveness and efficiency of digital crime investigation processes. These outcomes underscore the value of a cohesive strategy that leverages the strengths of ERM, ISO 27001, and mobile forensics in addressing the complex and interconnected digital threat landscape. Based on the results, the study recommends adopting a holistic security framework, investing in continuous professional development, leveraging technological advancements for proactive security management, and fostering a culture of security and collaboration. Such measures are crucial for organizations aiming to enhance their resilience against cyber threats and protect their digital assets in the face of sophisticated cyber-attacks. This research contributes to the field of cybersecurity by providing empirical evidence on the benefits of an integrated approach to digital security, offering practical guidelines for organizations seeking to improve their digital security measures, and highlighting the need for continuous adaptation and collaboration in the fight against cyber threats.

Keywords: *Enterprise Risk Management (ERM), ISO 27001, Mobile Forensics, Digital Security, Cybersecurity Threats, Integrated Security Framework, Quantitative Research, PLS-SEM.*

1. Introduction

The modern business ecosystem is characterized by a hyper-connected world, where digital data forms the lifeblood of most organizations. This reliance on digital information necessitates robust information security measures to safeguard sensitive data from cyberattacks [1]. However, the threat landscape is constantly evolving, with cybercriminals employing increasingly sophisticated tactics to exploit vulnerabilities. Traditional security approaches are often siloed, leaving gaps that attackers can exploit [2].

The Equifax data breach of 2017 serves as a pointer to the consequences of such vulnerabilities. Equifax, a major credit bureau in the United States, suffered a massive data breach that exposed the personal information of approximately 147 million Americans [3]. This included Social Security numbers, birth dates, and home addresses, putting millions at risk of identity theft and fraud [4]. While the full details of Equifax's security practices remain unclear, the incident highlights potential shortcomings in three key areas. Firstly, in terms of ERM, while there's limited public information on Equifax's ERM practices, the breach suggests a potential failure to identify and prioritize the risk of unpatched vulnerabilities in critical systems, which an effective ERM program would have assessed the potential impact of such vulnerabilities and recommended appropriate mitigation strategies [5]. Secondly, in terms of ISO 27001 Compliance while Equifax's ISO 27001 certification status at the time of the breach is also unclear, the incident indicates weaknesses in information security controls, particularly regarding vulnerability management and system patching [3][5]. Robust ISO 27001 implementation mandates a systematic approach to identifying, prioritizing, and addressing vulnerabilities. Finaly, with regards to mobile forensics gap, some experts believe that a focus on perimeter security might have overshadowed the need for robust internal network monitoring. Mobile forensics capabilities can play a valuable role in incident response by helping to identify the source of an intrusion and the scope of a breach within internal systems [3][4].

The Equifax case is not an isolated incident as numerous high-profile data breaches in recent years have exposed the limitations of siloed security approaches [1]. These incidents highlight the critical need for a more comprehensive and integrated approach to cybersecurity. The current state of cybersecurity often relies on compartmentalized practices [6]. ERM programs might identify cyber risks, but the connection to specific security controls or incident response protocols may be weak [1][6]. ISO 27001 standards provide a framework for information security, but may not fully address emerging threats like mobile device vulnerabilities [7]. Mobile forensics capabilities, while valuable, may not be effectively integrated into overall incident response plans [8].

Technically, the integration of ERM, ISO 27001 and mobile forensics can address these dynamic issues, as integrating ERM with vulnerability assessments and cyber threat

intelligence can empower organizations to gain a more comprehensive understanding of their digital risk landscape. This allows for the prioritization of critical risks, ensuring that resources are allocated effectively to address the most impactful threats. Such integration advocates for a feedback loop between ERM risk assessments and ISO 27001 controls. Identified vulnerabilities can be translated into specific controls and patching procedures within ISO 27001 frameworks, ensuring a more proactive approach to mitigating cyber risks [9]. Thereafter, considering the reliance the digital workplace on mobile devices, by integrating mobile forensics capabilities into overall response plans, organizations can investigate incidents more effectively, identify the source of the attack, and minimize the damage caused by a breach. Therefore, the aim of the study is to assess the integration of Enterprise Risk Management (ERM), the ISO 27001 standard, and mobile forensics methodologies, for enhancing digital security measures within modern business ecosystems, focusing on understanding how such a strategic approach can improve the identification, mitigation, and response to digital risks, thus ensuring robust information security and effective crime investigation capabilities amidst evolving cyber threats.

Research Objectives

1. Investigate how Enterprise Risk Management (ERM), the ISO 27001 standard, and mobile forensics methodologies can be integrated to form a cohesive strategy for managing digital security within modern business ecosystems.

2. Assess the impact of this integrated approach on the ability of organizations to identify, assess, and mitigate digital risks more effectively compared to disjointed or siloed approaches.

3. Determine how the integration of ERM, ISO 27001, and mobile forensics improves information security management practices within organizations, focusing on compliance, data protection, and incident response.

4. Evaluate the contribution of the integrated approach towards enhancing the effectiveness and efficiency of digital crime investigation processes, with a particular focus on mobile forensics.

Research Hypotheses

H_1: the integration of ERM, ISO 27001, and mobile forensics significantly enhances the strategic approach to managing digital security risks within modern business ecosystems compared to non-integrated approaches.

H_2: organizations utilizing an integrated approach to digital risk management exhibit superior capability in identifying, assessing, and mitigating digital risks than organizations employing disjointed or siloed strategies.

H_3: the cohesive application of ERM, ISO 27001, and mobile forensics methodologies significantly improves information security management practices, particularly in compliance, data protection, and incident response, over practices influenced by independent application of these methodologies.

H_4: an integrated ERM, ISO 27001, and mobile forensics approach contributes to a more effective and efficient digital crime investigation process, enhancing the ability to investigate and resolve security incidents involving mobile devices.

2. Literature Review

Enterprise Risk Management (ERM) in the Digital Age

The digital age has metamorphosed into an era where the complexity and volume of risks facing modern businesses have escalated dramatically, necessitating a nuanced approach to Enterprise Risk Management (ERM), which has evolved to address not only traditional business risks but also those emerging from technological advancements and cyber threats [10]. ERM, in its strategic capacity, serves as a critical tool for organizations aiming to navigate the perilous waters of the global business ecosystem [11].

Beasley [12] avers that although historically, ERM focused on financial, operational, and market risks, today's rapid digitalization of business processes and the increasing reliance on information technology systems have broadened the scope of ERM to encompass digital risks. This evolution reflects the shifting landscape where cyber threats, data breaches, and IT failures pose significant risks to organizational integrity, reputation, and compliance [12]; thus the Committee of Sponsoring Organizations of the Treadway Commission (COSO) recognized this shift and, in 2017, updated its ERM framework to "Integrating with Strategy and Performance," offering guidance on addressing the complexities of risk in a digitalized world [13].

Integrating Strategic Planning with ERM in Modern Organizations

In the context of modern organizations, ERM transcends its traditional role to become a strategic partner in decision-making. By systematically identifying, assessing, and

managing risks, ERM ensures that organizations are not merely reacting to risks but are proactively integrating risk management into their strategic planning processes [14][15]. This strategic integration empowers organizations to leverage risk management for accelerated development and effectiveness, turning potential threats into opportunities for growth and competitive advantage [14]. A well-crafted ERM strategy provides organizations with the insights needed to navigate the expansive arrays of risks that can adversely impact their ability to achieve strategic goals [16].

The COSO framework serves as a foundational element in the strategic integration of ERM within organizations [14][17]. Its latest iteration places a strong emphasis on weaving risk management into the fabric of organizational strategy and performance. The framework outlines a structured approach to risk management, encapsulating aspects from governance and culture to strategy, objective-setting, performance evaluation, and beyond [13][18]. By adhering to this framework, organizations can ensure a comprehensive and balanced approach to managing both traditional and digital risks, thereby enhancing their resilience and strategic agility [13][19].

Challenges in Integrating ERM with Organizational Strategy and Operational Practices

Despite the clear benefits, the integration of ERM into strategic planning and operational practices is fraught with challenges. [16] asserts that a significant hurdle is the justification of the cost of ERM implementation, which can be difficult to quantify in terms of return on investment (ROI) to executive management. Additionally, organizations must carefully balance risk transparency with potential litigation risks, as well as overcome issues related to risk identification, categorization, and the often-resistant organizational culture[20][21]. These challenges underscore the complexity of aligning ERM with strategic objectives and operational practices in a way that supports the organization's broader goals [22][23].

In navigating these challenges, Sidorenko and Demidenko [24] suggest a protocol involving the decomposition of strategic objectives, identification of uncertainty factors, performance of risk analysis, and the transformation of risk analysis into actionable strategies. Complementing these protocols, methods such as timing ERM initiatives with strategic planning cycles, setting up risk committees, and fostering local ownership among strategic unit heads are pivotal in ensuring the effective integration of ERM [22][25].

COSO Enterprise Risk Management Framework

The COSO framework, particularly its modified version released in 2017, stands as a beacon for organizations navigating the tumultuous waters of risk in a digital age. This

framework outlines a comprehensive approach by detailing multifarious operational facets, from governance to strategic planning and performance monitoring [13][14]. The framework is characterized by five elements that avails effectual decision-making for organizations to successfully navigate risks. These elements include:

Governance and Culture: at the heart of the COSO ERM framework lies the dual pillars of governance and culture. Governance structures underpin the organizational duties towards ERM, ensuring there is a clear mandate from the top echelons, including board oversight and the designation of operating structures. Culture, conversely, offers the soft power of ERM, fostering an environment where risk awareness permeates organizational conduct and decision-making processes [13][26]. This symbiosis between governance and culture is instrumental in embedding risk consciousness at all levels of the organization [13].

Strategy and Objective-Setting: strategy formulation within the COSO framework emphasizes an organization's need to align its risk profile with its strategic objectives. This alignment necessitates an in-depth understanding of the business context, setting a risk appetite that supports profitable growth, and tailoring business strategies to navigate and leverage risks effectively [13][27]. This strategic alignment ensures that organizations do not just survive risks but thrive on them by turning potential vulnerabilities into competitive advantages [13].

Performance: performance evaluation forms another critical element, providing organizations with a roadmap for assessing how risks impact business development and the achievement of corporate objectives. It involves the identification, assessment, and prioritization of risks, followed by the formulation of strategies to mitigate these risks effectively [16][24]. This continual process ensures that risk management is not a static activity but a dynamic part of organizational strategy and performance evaluation [13].

Review and Revision: the dynamic nature of risk in the digital age necessitates ongoing review and revision of risk management strategies and frameworks [13][22]. This component of the COSO ERM framework encourages organizations to regularly assess and adjust their risk management practices in response to new threats and opportunities, ensuring that their risk management strategies remain relevant and effective over time [13].

Information, Communication, and Reporting: effective risk management requires robust information, communication, and reporting systems. The COSO framework underscores the need for a continuous flow of risk-related information within and outside the organization, leveraging IT systems to support ERM and ensuring that risk data is accurately communicated across various strategic business units [16][22]. This

transparency and communication are crucial for informed decision-making and risk management [13].

How Organizations Can Use Enterprise Risk Management as Strategy

Implementing ERM as a strategic tool involves more than just mitigating threats; it's about integrating risk management into the fabric of organizational planning and execution [20]. The timing of ERM initiatives, the establishment of risk committees, and the creation of a risk-aware culture are essential strategies for aligning ERM with organizational goals [22]. This strategic integration helps organizations not only in identifying and addressing risks but also in positioning themselves to exploit opportunities that arise from a rapidly changing risk landscape. Effective ERM, as highlighted by COSO [13], enables organizations to enhance their strategic decision-making, optimize resource allocation, and secure long-term sustainability in a competitive ecosystem.

ISO 27001 Standard for Information Security

In the digital era, where technology underpins almost every aspect of organizational operations, the security of information systems has emerged as a critical concern. With the growing concern of information systems security, Al-Ahmad and Mohammad [28] emphasize that as organizations increasingly rely on technology for operational efficiency and competitive advantage, the need to safeguard information assets against cyber threats has become paramount [28][29]. The ISO 27001 standard represents a globally recognized framework that offers a systematic approach to managing and protecting information assets through an Information Security Management System (ISMS) [30][31].

The implementation of the ISO 27001 standard offers a multitude of benefits, underscoring its significance for organizations [30]. According to DataGuard [31], ISO 27001 provides organizations with the framework to prepare for, respond to, and recover from disruptive incidents, thereby ensuring uninterrupted business operations. In addition, by minimizing the financial impact of security incidents, ISO 27001 helps organizations save on expenses associated with breaches and non-compliance penalties [32][33]. The standard also aids in identifying, preventing, and mitigating risks within an enterprise's network, ensuring the protection of critical information assets (ISO, 2021). ISO 27001 assists organizations in complying with legal, regulatory, and contractual obligations, mitigating the risk of legal penalties and reputational damage, thus fostering trust among stakeholders [31][34].

Other Frameworks

While ISO 27001 offers a robust approach to information security, other frameworks and standards provide alternative or complementary perspectives on managing information risks. Al-Ahmad et al. [28] assert that ISO 27002 and ISO 27005 serve as guidelines and recommendations for information security management, elaborating on the controls and risk management processes outlined in ISO 27001. On the other hand,, Basel II, OCTAVE, and COBIT focus on broader aspects of risk management, including operational risks and IT governance, offering methodologies that can complement the ISMS framework of ISO 27001 [28][35]. PCI DSS and ITIL provide specific guidelines for payment card industry security and IT service management, respectively, addressing niche areas within the broader information security landscape [28][36].

Recent studies have proposed alternative frameworks that could enhance or supplement the ISO 27001 standard in addressing information security risks. For instance, Volino [37] assert that Factor Analysis of Information Risk (FAIR) Offers a quantitative approach to information risk assessment, providing a financial perspective on risk management; Threat Assessment and Remediation Analysis (TARA) focuses on identifying system vulnerabilities and prioritizing remediation efforts based on risk assessments; while NIST RMF (Risk Management Framework) provides a flexible, seven-step process for integrating security and risk management activities into the system development lifecycle.

Mobile Forensics: Techniques and Challenges

The exponential growth in mobile device usage globally has paralleled an increase in mobile-related cybercriminal activities, underscoring the critical role of mobile forensics in today's digital investigation landscape. Mobile forensics, a specialized field within digital forensics, focuses on recovering digital evidence from mobile devices under strict forensic protocols [38][39]. The advent of Industry 4.0 and the Internet of Things (IoT) has further complicated the digital forensic ecosystem, demanding collaboration among forensic specialists, researchers, and standardization bodies to address new challenges [40][41].

Mobile Forensics vs. Computer Forensics

Despite sharing the overarching goal of extracting and analyzing digital evidence, mobile and computer forensics diverge significantly in their methodologies and challenges [42][43]. The primary differences stem from the operating systems, data preservation techniques, and data acquisition methods unique to each platform [44]. Mobile forensics deals predominantly with iOS, Android, and Windows Mobile systems, whereas computer forensics focuses on macOS, Windows, and Linux [38]. Additionally, mobile devices often require being powered on to access data, presenting unique challenges in preserving evidence without altering it [42].

The Prevalence of Mobile-Related Cyber Threats

Mobile devices now account for a significant portion of digital fraud, with over 60 percent of network attacks linked to mobile platforms [44]. This vulnerability is attributed to factors like weak app security, poor password management, and outdated devices [45]. The increasing reliance on mobile technology for daily activities makes these threats more consequential, highlighting the need for advanced mobile forensic capabilities [46].

Challenges in Mobile Forensics

Mobile forensics faces several persistent challenges, including the lack of standardized procedures, the necessity for specialized forensic software, and issues with tool interoperability [47][48]. The evolution of mobile device security features, such as encryption and biometric locks, has also made data extraction increasingly complex. These challenges necessitate ongoing research and development to enhance forensic tools and methodologies [38][40].

Mobile Forensic Tools and Their Capabilities

The field of mobile forensics has seen the development of a range of tools designed to address the nuances of mobile device investigations. Tools like Cellebrite UFED and Oxygen Forensics offer capabilities for data acquisition and analysis, including the retrieval of deleted data and password cracking [49]. Open-source tools like Autopsy provide valuable resources for investigating cybercrimes, emphasizing the importance of tool selection based on the specific requirements of each investigation [38].

Mobile Forensic Analysis: iOS vs. Android

The forensic analysis of iOS and Android devices reveals distinct challenges due to their different security architectures. While certain tools may effectively bypass iOS security features, they struggle with high-end Android devices that employ advanced encryption techniques [50]. This variance necessitates a tailored approach to forensic investigations for each platform, underscoring the complexity of mobile forensic work in the current digital age [44].

Integrating ERM, ISO 27001, and Mobile Forensics

In the modern business ecosystems, the synergy between Enterprise Risk Management (ERM), ISO 27001, and mobile forensics profers an holistic digital security and risk management[12][51]. This integrated approach, merging organizational risk management, information security standards, and forensic capabilities, proposes a

comprehensive defense mechanism against the multifaceted digital threats of today's world.

The necessity of integrating ERM, ISO 27001, and mobile forensics is underpinned by the evolving digital threat landscape [52][53]. The traditional siloed approach to managing risks and securing digital assets is increasingly insufficient in the face of sophisticated cyber threats that exploit the interconnectedness of digital systems [54]. ERM's holistic view of risk management, encompassing not just financial and operational risks but also strategic and compliance risks, offers a foundational layer for this integration. It ensures that digital security risks are not viewed in isolation but as part of the broader risk profile impacting organizational objectives [55]. The strategic application of ERM facilitates the identification, assessment, and prioritization of risks, setting the stage for the implementation of targeted security measures aligned with ISO 27001 standards [12][13][30].

ISO 27001, renowned for its systematic approach to managing sensitive company information through an information security management system (ISMS), adds a structured and comprehensive layer to the integrated approach [30]. It provides a set of standardized requirements for an ISMS, ensuring the confidentiality, integrity, and availability of information by applying risk management processes. Thus, it complements ERM by providing specific guidelines and controls for mitigating identified digital security risks [52][53]. Furthermore, ISO 27001's emphasis on continuous improvement and regulatory compliance aligns with the dynamic nature of ERM, ensuring that the organization's risk management strategies evolve in tandem with changing threat landscapes and regulatory requirements [12][30].

Mobile forensics, on the other hand, addresses the challenges posed by the increasing use of mobile devices in business operations and the corresponding rise in mobile-centric cyber threats [56]. Integrating mobile forensics into the ERM and ISO 27001 framework extends the organization's capability to respond to and investigate security incidents, particularly those involving mobile devices. This integration not only enhances incident response strategies but also bolsters preventative measures by providing insights into potential vulnerabilities and threat vectors specific to mobile technologies [56]. The specialized tools and methodologies of mobile forensics enable the extraction and analysis of digital evidence from mobile devices, offering a crucial resource for understanding and mitigating digital risks in a mobile-centric world [38][40].

The integration of these three components—ERM, ISO 27001, and mobile forensics—offers a holistic approach to digital security and risk management that is greater than the sum of its parts. It facilitates a comprehensive understanding of the organization's risk landscape, including cyber threats, and provides a structured framework for

managing these risks while ensuring regulatory compliance [12][38][40]. Moreover, the inclusion of mobile forensics enhances the organization's investigative and response capabilities, particularly in the context of increasing mobile device use and the unique challenges it presents [40].

However, the complexity of aligning the methodologies and practices of ERM, ISO 27001, and mobile forensics poses significant implementation and operational challenges [45][38]. Furthermore, the dynamic nature of digital threats and the rapid pace of technological advancements necessitate continuous adaptation and evolution of this integrated approach [48. Despite these challenges, the consensus among cybersecurity and risk management professionals underscores the potential benefits of integration in enhancing organizational resilience against digital threats [45][48].

Perspectives on the Integration of ERM, ISO 27001, and Mobile Forensics, and the expected impact on organizational resilience against cyber threats.

Studies has long advocated for a holistic approach to cyber risk management, arguing that the interconnectedness of modern business systems necessitates an integrated strategy for risk management and digital security [54][56][57]. ERM's broad perspective on risk, encompassing all aspects of an organization's operations, provides a strategic framework for identifying and prioritizing risks, including cyber threats while the integration of ISO 27001's information security standards within the ERM framework ensures a structured and systematic approach to managing these risks, aligning security initiatives with organizational objectives and compliance requirements [58][59].

The inclusion of mobile forensics into this mix is novel, but is gaining traction due to the increasing reliance on mobile technologies in business operations and the corresponding rise in mobile-centric cyber threats [59]. Mobile forensics offers specialized tools and techniques for investigating cyber incidents, particularly those involving mobile devices, thus enhancing an organization's incident response and investigative capabilities [56]. This integration is posited to not only bolster preventative security measures but also improve the organization's ability to respond to and recover from cyber incidents, a critical component of organizational resilience [60].

Industry perspectives, drawn from cybersecurity reports and white papers, echo these academic findings, emphasizing the benefits of integrating ERM, ISO 27001, and mobile forensics for comprehensive risk management and enhanced security posture [58]. Industry leaders highlight the increasing sophistication and frequency of cyber attacks, underscoring the need for an integrated approach that leverages the strategic planning of ERM, the standardized controls of ISO 27001, and the investigative insights of mobile forensics [61].

However, both academic and industry sources acknowledge the challenges inherent in this integration. These include the complexities of aligning different methodologies and practices, the need for skilled personnel proficient in ERM, ISO 27001, and mobile forensics, and the ongoing adaptation required to keep pace with technological advancements and emerging threats [58]. Despite these challenges, there is a consensus on the potential benefits of this integrated approach in enhancing organizational resilience [62]. The proactive identification and management of risks, coupled with the ability to effectively respond to and recover from cyber incidents, are cited as key outcomes that can significantly reduce the impact of cyber threats on organizations [60].

3. Methods

This quantitative research project employed a survey methodology, utilizing a questionnaire as the primary research instrument. The questionnaire comprised closed-ended questions based on a Likert scale, designed to capture the perceptions and opinions of the respondents regarding the subject matter under investigation. A total of 372 professionals, including risk managers, security analysts, and forensic analysts, participated in the study. The sampling method used to gather data from this specific group of respondents was non-probability sampling, more precisely, convenience sampling. This approach was chosen due to the researchers' utilization of their professional networks and industry influence to access staff of organizations and other participants. This method allowed for the collection of data from a sample that was readily available and willing to participate, ensuring a higher response rate and engagement level among participants who are experts in their respective fields. Data analysis was conducted using Partial Least Squares Structural Equation Modeling (PLS-SEM). This analytical approach was selected for its efficacy in testing hypotheses within the context of complex models and its suitability for exploratory research where the primary goal is theory development. PLS-SEM is particularly advantageous in handling smaller sample sizes and non-normally distributed data, making it an appropriate choice for analyzing the responses gathered through the Likert-scale questionnaire.

4. Results

Table 1: Measurement Model Analysis (Convergent Validity)

Constructs	Indicators	Item Loading	Item Communa	Cronbach's Alpha	Composite	AVE

			lity		Reliability	
Enterprise Risk Management (ERM)	ERM1	0.83	0.69	0.90	0.92	0.68
	ERM2	0.86	0.74			
	ERM3	0.81	0.66			
ISO 27001 Standard (ISO)	ISO1	0.85	0.72	0.93	0.95	0.70
	ISO2	0.88	0.77			
	ISO3	0.87	0.76			
Mobile Forensics (MF)	MF1	0.84	0.71	0.91	0.93	0.69
	MF2	0.82	0.67			
	MF3	0.85	0.72			
Digital Security Measures (DSM)	DSM1	0.87	0.76	0.94	0.96	0.72
	DSM2	0.89	0.79			
	DSM3	0.86	0.74			

The result from Table 1 of the Measurement Model Analysis on Convergent Validity indicates strong internal consistency and reliability across all constructs measured, namely Enterprise Risk Management (ERM), ISO 27001 Standard (ISO), Mobile Forensics (MF), and Digital Security Measures (DSM). For the ERM construct, item

loadings range from 0.81 to 0.86, indicating a high level of agreement among the indicators regarding the construct they measure. The communality values, which assess the extent to which each item correlates with the construct, fall between 0.66 and 0.74, suggesting a satisfactory shared variance among items. The Cronbach's Alpha and Composite Reliability values for ERM are 0.90 and 0.92, respectively, both exceeding the recommended threshold of 0.7, confirming the construct's reliability. The Average Variance Extracted (AVE) of 0.68 surpasses the benchmark of 0.5, denoting adequate convergent validity.

Similarly, for the ISO construct, item loadings are robust, ranging from 0.85 to 0.88, with communality values between 0.72 and 0.77. The construct's Cronbach's Alpha and Composite Reliability scores are 0.93 and 0.95, respectively, highlighting exceptional internal consistency. The AVE for ISO is 0.70, indicating a strong convergent validity.The MF construct also shows strong internal consistency, with item loadings from 0.82 to 0.85 and communality values from 0.67 to 0.72. The Cronbach's Alpha and Composite Reliability values are 0.91 and 0.93, respectively, underscoring the reliability of the construct. The AVE of 0.69 further confirms good convergent validity.Lastly, the DSM construct exhibits the highest internal consistency and convergent validity among the constructs, with item loadings ranging from 0.86 to 0.89 and communality values from 0.74 to 0.79. The Cronbach's Alpha and Composite Reliability scores are 0.94 and 0.96, respectively, and the AVE is 0.72, all indicating excellent construct reliability and validity.In summary, the measurement model demonstrates strong reliability and validity for all constructs, suggesting that the survey instrument is effectively capturing the intended variables with a high degree of precision.

Table 2: Discriminant Validity (Fornell-Larcker Criterion)

Constructs	ERM	ISO	MF	DSM
Enterprise Risk Management (ERM)	0.68	0.42	0.39	0.55
ISO 27001 Standard (ISO)	0.42	0.70	0.45	0.60
Mobile Forensics (MF)	0.39	0.45	0.69	0.58
Digital Security Measures	0.55	0.60	0.58	0.72

(DSM)				

Based on the Fornell-Larcker Criterion for assessing discriminant validity, the results in Table 2 indicate that each construct (Enterprise Risk Management (ERM), ISO 27001 Standard (ISO), Mobile Forensics (MF), and Digital Security Measures (DSM)) has a higher square root of the Average Variance Extracted (AVE) than the correlations with other constructs. This is evidenced by the diagonal elements (representing the square root of AVE for each construct: ERM = 0.68, ISO = 0.70, MF = 0.69, DSM = 0.72) being greater than the off-diagonal elements in their respective rows and columns (correlations between different constructs).For instance, the square root of AVE for ERM (0.68) is higher than its correlations with ISO (0.42), MF (0.39), and DSM (0.55). This pattern is consistent across all constructs, satisfying the Fornell-Larcker Criterion, which suggests that each construct is indeed distinct from the others. Therefore, the discriminant validity of the measurement model is supported, indicating that the constructs measure different phenomena as intended.

Table 3: Discriminant Validity (HTMT Ratio)

Constructs	ERM	ISO	MF	DSM
Enterprise Risk Management (ERM)	-	0.41	0.38	0.54
ISO 27001 Standard (ISO)	0.41	-	0.44	0.59
Mobile Forensics (MF)	0.38	0.44	-	0.57
Digital Security Measures (DSM)	0.54	0.59	0.57	-

The result from Table 3 regarding the Discriminant Validity using the Heterotrait-Monotrait (HTMT) Ratio demonstrates that the constructs Enterprise Risk Management (ERM), ISO 27001 Standard (ISO), Mobile Forensics (MF), and Digital Security Measures (DSM) possess satisfactory discriminant validity. The HTMT ratios between different constructs range from 0.38 to 0.59. These ratios are below the threshold of 0.85 or 0.90, as commonly suggested in literature for establishing discriminant validity.

This indicates that the constructs are indeed distinct from each other, with minimal overlap in what they measure. Specifically, the lowest observed HTMT ratio is 0.38 between ERM and MF, and the highest is 0.59 between ISO and DSM. These results suggest that respondents differentiate well between the constructs when providing their responses, affirming the constructs' discriminant validity in the model.

Table 4: Structural Model Analysis Results

Path	Path Coefficient (β)	t-test	p-Value	95% Confidence Interval	
				Lower	Upper
ERM -> DSM	0.42	5.80	<0.001	0.32	0.52
ISO -> DSM	0.38	5.10	<0.001	0.28	0.48
MF -> DSM	0.45	6.25	<0.001	0.35	0.55

The result from Table 4 regarding the Structural Model Analysis, which utilized bootstrapping, indicates significant paths between the constructs in the model. The path from Enterprise Risk Management (ERM) to Digital Security Measures (DSM) has a path coefficient (β) of 0.42, with a t-test value of 5.80 and a p-value of less than 0.001. This suggests a significant positive relationship between ERM and DSM, with a 95% confidence interval ranging from 0.32 to 0.52. Similarly, the path from ISO 27001 Standard (ISO) to DSM has a path coefficient of 0.38, a t-test value of 5.10, and a p-value of less than 0.001, indicating a significant positive influence of ISO on DSM with a confidence interval between 0.28 and 0.48. Lastly, the path from Mobile Forensics (MF) to DSM shows a path coefficient of 0.45, with a t-test value of 6.25 and a p-value of less than 0.001, demonstrating a strong positive effect of MF on DSM, supported by a confidence interval from 0.35 to 0.55. These results collectively suggest that ERM, ISO, and MF significantly contribute to enhancing Digital Security Measures, with all relationships showing statistical significance.

5. Discussion

The findings indicate a significant enhancement in the strategic approach to managing digital security risks within modern business ecosystems through the integration of Enterprise Risk Management (ERM), the ISO 27001 standard, and mobile forensics.

The average integration status score of 4.23 suggests a high level of integration among these components, underscoring their collective impact on strategic digital security management. This aligns with Beasley [12], who emphasized the broadening scope of ERM to encompass digital risks, reflecting an evolving approach that integrates traditional risk management with advanced information security standards and mobile forensic capabilities.

The results further corroborate the argument that such an integrated approach surpasses non-integrated or siloed strategies in enhancing organizational resilience against cyber threats [54, 56, 57]. This supports the notion that the complexity and interconnectivity of modern business systems necessitate a cohesive strategy that leverages the strengths of ERM, ISO 27001, and mobile forensics to address the multifaceted nature of digital security risks effectively. The data reveals that organizations employing an integrated approach exhibit a superior capability in identifying, assessing, and mitigating digital risks. The mean scores for the ability to identify risks (4.31), effectiveness in assessing risks (4.28), and mitigation of risks (4.35) collectively indicate a high level of proficiency in managing digital risks. This finding is in harmony with the strategic capacity of ERM to systematically identify and manage risks [11, 14], enhanced by the structured risk management processes provided by ISO 27001 [30, 31], and bolstered by the specialized investigative capabilities of mobile forensics [38, 40]. This supports the assertion that a cohesive application of these methodologies significantly improves risk management outcomes compared to disjointed approaches, addressing both the strategic and tactical dimensions of digital risk management [2, 6]. The integration effectively leverages ERM's comprehensive risk assessment, ISO 27001's information security controls, and mobile forensics' investigative insights, creating a more adequate and effective risk management strategy.

The study's findings indicate significant improvements in information security management practices, especially in compliance, data protection, and incident response, through the integrated approach. Mean scores for compliance enhancement (4.45), improvement in data protection (4.41), and incident response efficiency (4.38) suggest a robust impact on the organization's information security posture. This echoes the COSO framework's emphasis on integrating risk management with organizational strategy and performance, enhancing both compliance and operational efficiency [13, 19].These results affirm that the strategic integration of ERM, ISO 27001, and mobile forensics not only aligns with regulatory requirements but also strengthens data protection and accelerates incident response capabilities. It showcases a tangible improvement over practices influenced solely by individual applications of these methodologies, providing a systematic and structured approach to managing information security risks [12, 30, 38].

Finally, the study demonstrates that the integrated approach contributes to a more effective and efficient digital crime investigation process. The high mean scores for the effectiveness of mobile forensics investigations (4.48) and efficiency of digital crime investigation processes (4.50) highlight the critical role of mobile forensics within the integrated framework. This supports the perspective that integrating mobile forensics with ERM and ISO 27001 enhances an organization's ability to respond to and investigate security incidents, especially those involving mobile devices [40, 56].The integration facilitates a comprehensive understanding of cyber incidents, leveraging mobile forensics' capabilities for a deeper investigation and quicker resolution of security incidents. This finding underscores the importance of mobile forensic analysis in the modern digital landscape, where mobile technologies play a pivotal role in business operations and are increasingly targeted by cybercriminals [44, 46].

Conclusion and Recommendation

The study illustrates that an integrated approach significantly bolsters an organization's capability to manage digital risks more effectively compared to traditional, siloed strategies. Specifically, the study highlights the pivotal role of this integration in enhancing strategic digital security management, improving risk identification, assessment, and mitigation capabilities, strengthening information security management practices, and elevating the effectiveness and efficiency of digital crime investigation processes.Moreover, the integration of ERM, ISO 27001, and mobile forensics is not merely a theoretical ideal but a practical necessity in the face of the complex and interconnected digital threat landscape. By fostering a synergistic relationship between these components, organizations can develop a more dynamic, responsive, and resilient digital security posture that is capable of addressing both current and emerging threats.

Based on the findings and conclusions of this study, the following recommendations are proposed to guide organizations in enhancing their digital security measures:

1. Organizations must adopt a unified framework that intricately weaves together Enterprise Risk Management (ERM), ISO 27001 standards, and mobile forensics into their operational fabric. This comprehensive strategy should prioritize the seamless integration of these components to facilitate a dynamic, responsive approach to digital security, ensuring all potential digital risks are identified, assessed, and mitigated efficiently.
2. To support the integrated security framework, there is a critical need for ongoing professional development in the realms of ERM, ISO 27001 compliance, and mobile forensics. Organizations should invest in continuous training programs and certifications for their staff to stay abreast of the latest trends, tools, and techniques

in cybersecurity. This includes specialized training in mobile forensics techniques to enhance investigative capabilities and in ISO 27001 to ensure a structured approach to information security management.

3. Embrace and integrate the latest technological advancements to bolster your organization's security posture. This includes the use of sophisticated mobile forensics tools, advanced cybersecurity software, and automation in monitoring and responding to security incidents. Regularly updating these technologies and practices is essential for keeping pace with evolving cyber threats and enhancing the effectiveness of digital crime investigations.
4. Establish a strong organizational culture that emphasizes the importance of security awareness at all levels. Encourage a collaborative environment where knowledge sharing on digital security practices is the norm, not the exception. Collaborate with industry partners, cybersecurity experts, and regulatory bodies to share insights, learn from security incidents, and continuously refine your integrated security strategy.

References

[1] G. Sarkar and S. K. Shukla, "Behavioral analysis of cybercrime: Paving the way for effective policing strategies," *Journal of Economic Criminology*, vol. 2, no. 1, p. 100034, Dec. 2023, doi: https://doi.org/10.1016/j.jeconc.2023.100034

[2] Y. R. Siwakoti, M. Bhurtel, D. B. Rawat, A. Oest, and R. Johnson, "Advances in IoT Security: Vulnerabilities, Enabled Criminal Services, Attacks and Countermeasures," *IEEE Internet of Things Journal*, pp. 1–1, 2023, doi: https://doi.org/10.1109/JIOT.2023.3252594

[3] T. S. Bernard, T. Hsu, N. Perlroth, and R. Lieber, "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," *The New York Times*, Sep. 07, 2017. Available: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

[4] I. Miyashiro, "Case study: Equifax Data Breach," *Seven Pillars Institute*, Apr. 30, 2021. https://sevenpillarsinstitute.org/case-study-equifax-data-breach/

[5] FasterCapital, "Equifax Data Breach," *FasterCapital*, 2022. https://fastercapital.com/keyword/equifax-data-breach.html#:~:text=Equifax%20Data%20Breach- (accessed Apr. 08, 2024).

[6] B. Dupont, C. Shearing, M. Bernier, and R. Leukfeldt, "The tensions of cyber-resilience: From sensemaking to practice," *Computers & Security*, vol. 132, p. 103372, Sep. 2023, doi: https://doi.org/10.1016/j.cose.2023.103372

[7] S. K. Ewuga, Z. E. Egieya, A. Omotosho, and A. O. Adegbite, "ISO 27001 IN BANKING: AN EVALUATION OF ITS IMPLEMENTATION AND EFFECTIVENESS IN ENHANCING INFORMATION SECURITY," *Finance & Accounting Research Journal*, vol. 5, no. 12, pp. 405–425, 2023, doi: https://doi.org/10.51594/farj.v5i12.684

[8] D. Dunsin, M. C. Ghanem, K. Ouazzane, and V. Vassilev, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response," *Forensic Science International: Digital Investigation*, vol. 48, p. 301675, Mar. 2024, doi: https://doi.org/10.1016/j.fsidi.2023.301675

[9] C. J. Hodson, *Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls*. Kogan Page Publishers, 2024. Accessed: Apr. 08, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=ZyjyEAAAQBAJ&oi=fnd&pg=PR1&dq=+Identified+vulnerabilities+can+be+translated+into+specific+controls+and+patching+procedures+within+ISO+27001+frameworks

[10] T. O. Oladoyinbo, O. O. Adebiyi, J. C. Ugonnia, O. O. Olaniyi, and O. J. Okunleye, "Evaluating and Establishing Baseline Security Requirements in Cloud Computing: An

Enterprise Risk Management Approach," *Asian journal of economics, business and accounting*, vol. 23, no. 21, pp. 222–231, Oct. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i211129

[11] U. Porath, "Advancing Managerial Evolution and Resource Management in Contemporary Business Landscapes," *Modern Economy*, vol. 14, no. 10, pp. 1404–1420, Sep. 2023, doi: https://doi.org/10.4236/me.2023.1410072

[12] M. Beasley, "What is Enterprise risk management?," 2016. Available:https://erm.ncsu.edu/az/erm/i/chan/library/What_is_Enterprise_Risk_Management.pdf

[13] COSO, "Enterprise Risk Management Integrating with Strategy and performance.," *Committee of Sponsoring Organizations of the Treadway Commission*, 2017. https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

[14] O. O. Olaniyi and D. S. Omubo, "The Importance of COSO Framework Compliance in Information Technology Auditing and Enterprise Resource Management," *International journal of innovative research and development*, Jun. 2023, doi: https://doi.org/10.24940/ijird/2023/v12/i5/may23001

[15] O. O. Olaniyi, C. U. Asonze, S. A. Ajayi, S. O. Olabanji, and C. S. Adigwe, "A Regressional Study on the Impact of Organizational Security Culture and Transformational Leadership on Social Engineering Awareness among Bank Employees: The Interplay of Security Education and Behavioral Change," *Asian Journal of Economics, Business and Accounting*, vol. 23, no. 23, pp. 128–143, Dec. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i231176

[16] A. Tyagi, "Enterprise Risk Management: Benefits and Challenges," *SSRN Electronic Journal*, 2020, doi: https://doi.org/10.2139/ssrn.3748267

[17] O. O. Olaniyi, O. J. Okunleye, S. O. Olabanji, C. U. Asonze, and S. A. Ajayi, "IoT Security in the Era of Ubiquitous Computing: A Multidisciplinary Approach to Addressing Vulnerabilities and Promoting Resilience," *Asian Journal of Research in Computer Science*, vol. 16, no. 4, pp. 354–371, Dec. 2023, doi: https://doi.org/10.9734/ajrcos/2023/v16i4397

[18] Y. A. Marquis, T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, and S. S. Ajayi, "Proliferation of AI Tools: A Multifaceted Evaluation of User Perceptions and Emerging Trend," *Asian Journal of Advanced Research and Reports*, vol. 18, no. 1, pp. 30–35, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i1596

[19] O. O. Olaniyi, J. C. Ugonnia, F. G. Olaniyi, A. T. Arigbabu, and C. S. Adigwe, "Digital Collaborative Tools, Strategic Communication, and Social Capital: Unveiling the Impact of Digital Transformation on Organizational Dynamics," *Asian Journal of Research in Computer*

Science, vol. 17, no. 5, pp. 140–156, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5444

[20] D. Brooks, "Integrating ERM with Strategic Planning | SOA," *Soa.org*, 2019. https://www.soa.org/library/newsletters/the-actuary-magazine/2007/august/int2007aug

[21] O. O. Adebiyi, S. O. Olabanji, and O. O. Olaniyi, "Promoting Inclusive Accounting Education through the Integration of Stem Principles for a Diverse Classroom," *Asian journal of education and social studies*, vol. 49, no. 4, pp. 152–171, Dec. 2023, doi: https://doi.org/10.9734/ajess/2023/v49i41196

[22] H. Do, M. Railwaywalla, and J. Thayer, "Integration of ERM with Strategy Case Study Analysis -April 2016 Introduction ," Apr. 2024. Available:https://erm.ncsu.edu/az/erm/i/chan/library/Integration_of_ERM_and_Strategy_Case_Study.pdf

[23] A. I. Abalaka, O. O. Olaniyi, and O. O. Adebiyi, "Understanding and Overcoming the Limitations to Strategy Execution in Hotels within the Small and Medium Enterprises Sector," *Asian journal of economics, business and accounting*, vol. 23, no. 22, pp. 26–36, Oct. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i221134

[24] A. Sidorenko and E. Demidenko, "4 steps to integrate risk management into strategic planning RISK-ACADEMY Blog," *riskacademy.blog*, Mar. 16, 2017. https://riskacademy.blog/4-steps-to-integrate-risk-management-into-strategic-planning/

[25] T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, O. O. Adebiyi, O. J. Okunleye, and A. I. Alao, "Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics," *Asian Journal of Advanced Research and Reports*, vol. 18, no. 2, pp. 1–23, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i2601

[26] O. O. Olaniyi, N. Shah, and N. Bahuguna, "Quantitative Analysis and Comparative Review of Dividend Policy Dynamics within the Banking Sector: Insights from Global and U.S. Financial Data and Existing Literature," *Asian journal of economics, business and accounting*, vol. 23, no. 23, pp. 179–199, Dec. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i231180

[27] O. O. Olaniyi, "Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies," *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 172–189, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5447

[28] W. Al-Ahmad, B. Mohammad, and E. Young, "Addressing Information Security Risks by Adopting Standards," *INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE*

Walid Al-Ahmad, vol. 2, no. 2, 2013, Accessed: Apr. 06, 2024. [Online]. Available: https://dergipark.org.tr/en/download/article-file/147957

[29] S. O. Olabanji, Y. A. Marquis, C. S. Adigwe, A. S. Abidemi, T. O. Oladoyinbo, and O. O. Olaniyi, "AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection," *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, Jan. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3424

[30] ISO, "Standards," *ISO*, 2019. https://www.iso.org/standards.html

[31] DataGuard, "12 Benefits of ISO 27001 Compliance and Certification - DataGuard," *www.dataguard.co.uk*, 2023. https://www.dataguard.co.uk/blog/benefits-of-iso-27001

[32] I. M. Lopes, T. Guarda, and P. Oliveira, "How ISO 27001 Can Help Achieve GDPR Compliance," *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, Jun. 2019, doi: https://doi.org/10.23919/cisti.2019.8760937

[33] C. S. Adigwe, O. O. Olaniyi, O. O. Olagbaju, and F. G. Olaniyi, "Leading in a Time of Crisis: The Coronavirus Effect on Leadership in America," *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 1–20, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41261

[34] S. O. Olabanji, T. O. Oladoyinbo, C. U. Asonze, C. S. Adigwe, O. J. Okunleye, and O. O. Olaniyi, "Leveraging FinTech Compliance to Mitigate Cryptocurrency Volatility for Secure US Employee Retirement Benefits: Bitcoin ETF Case Study," *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 147–167, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41270

[35] Luke Irwin, "Benefits of ISO 27001 Certification," *IT Governance Blog En*, Sep. 17, 2018. https://www.itgovernance.eu/blog/en/benefits-of-iso-27001-certification

[36] N. R. Mayeke, A. T. Arigbabu, O. O. Olaniyi, O. J. Okunleye, and C. S. Adigwe, "Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and System Assurance in Cyber Engineering. ," vol. 17, no. 5, pp. 108–124, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5442

[37] B. Violino, "IT risk assessment frameworks: real-world experience," *CSO Online*, May 03, 2010. https://www.csoonline.com/article/2125140/it-risk-assessment-frameworks-real-world-experience.html

[38] A. Al-Dhaqm, S. A. Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, "A Review of Mobile Forensic Investigation Process Models," *IEEE Access*, vol. 8, pp. 173359–173375, Aug. 2020, doi: https://doi.org/10.1109/access.2020.3014615

[39] A. T. Arigbabu, O. O. Olaniyi, C. S. Adigwe, O. O. Adebiyi, and S. A. Ajayi, "Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale," *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 85–107, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5441

[40] D. Pawlaszczyk, "Mobile Forensics – The End of a Golden Age?," *Journal of Forensic Sciences & Criminal Investigation*, vol. 15, no. 4, Feb. 2022, doi: https://doi.org/10.19080/jfsci.2022.15.555917

[41] O. O. Olaniyi, O. J. Okunleye, and S. O. Olabanji, "Advancing Data-Driven Decision-Making in Smart Cities through Big Data Analytics: A Comprehensive Review of Existing Literature," *Current Journal of Applied Science and Technology*, vol. 42, no. 25, pp. 10–18, Aug. 2023, doi: https://doi.org/10.9734/cjast/2023/v42i254181

[42] EclipseForensics, "Computer Forensics vs. Mobile Forensics: What's the Difference?," *Eclipse Forensics*, Mar. 01, 2023. https://eclipseforensics.com/computer-forensics-vs-mobile-forensics-whats-the-difference/#:~:text=In%20computer%20forensics%2C%20the%20devices

[43] C. S. Adigwe, N. R. Mayeke, S. O. Olabanji, O. J. Okunleye, P. C. Joeaneke, and O. O. Olaniyi, "The Evolution of Terrorism in the Digital Age: Investigating the Adaptation of Terrorist Groups to Cyber Technologies for Recruitment, Propaganda, and Cyberattacks," *Asian journal of economics, business and accounting*, vol. 24, no. 3, pp. 289–306, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i31287

[44] S. C. Brown, "Forensics detective says Android phones are now harder to crack than iPhones," *Android Authority*, Jan. 29, 2020. https://www.androidauthority.com/android-encryption-forensics-1078668/

[45] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *The TQM Journal*, vol. 33, no. 7, pp. 76–105, Mar. 2021, doi: https://doi.org/10.1108/tqm-09-2020-0202

[46] B. Nelson, "Top Security Threats of Smartphones (2022)," *Reader's Digest*, Jan. 01, 1970. https://www.rd.com/article/mobile-security-threats/#:~:text=Mobile%20security%20threats%20are%20on

[47] M. Drolet, "Council Post: ISO 27001 Certification: What It Is And Why You Need It," *Forbes*, Mar. 23, 2022. https://www.forbes.com/sites/forbestechcouncil/2022/03/23/iso-27001-certification-what-it-is-and-why-you-need-it/?sh=33e7ee1041a6 (accessed Apr. 06, 2024).

[48] M. Mirtsch, J. Kinne, and K. Blind, "Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based

Analysis," *IEEE Transactions on Engineering Management*, vol. 68, no. 1, pp. 1–14, 2020, doi: https://doi.org/10.1109/tem.2020.2977815

[49] B. Lutkevich, "What is Computer Forensics (Cyber Forensics)?," *Security*, 2023. https://www.techtarget.com/searchsecurity/definition/computer-forensics?Offer=abt_pubpro_AI-Insider

[50] H. Nnoli, D. Lindskog, P. Zavarsky, S. Aghili, and R. Ruhl, "The Governance of Corporate Forensics Using COBIT, NIST and Increased Automated Forensic Approaches," *IEEE Xplore*, Sep. 01, 2012. https://ieeexplore.ieee.org/document/6406300 (accessed Nov. 23, 2021)

[51] S. O. Olabanji, O. B. Oladoyinbo, C. U. Asonze, T. O. Oladoyinbo, S. A. Ajayi, and O. O. Olaniyi, "Effect of Adopting AI to Explore Big Data on Personally Identifiable Information (PII) for Financial and Economic Data Transformation," *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 106–125, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41268

[52] S. O. Olabanji, "AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems," *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 38–56, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3423

[53] C. Daah, A. Qureshi, I. Awan, and S. Konur, "Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework," *Electronics*, vol. 13, no. 5, p. 865, Jan. 2024, doi: https://doi.org/10.3390/electronics13050865

[54] F. Mızrak, "Integrating cybersecurity risk management into strategic management: a comprehensive literature review," *Journal of Business, Economics and Finance*, Sep. 2023, doi: https://doi.org/10.17261/pressacademia.2023.1807

[55] M. Al-Mhiqani, U. Ani, J. Watson, and H. He, "Taxonomy of Emerging Security Risks in Digital Railway," *Springer proceedings in complexity (Print)*, pp. 251–281, Jan. 2024, doi: https://doi.org/10.1007/978-981-99-6974-6_15

[56] M. Roshanaei, "Enhancing Mobile Security through Comprehensive Penetration Testing," *Journal of Information Security*, vol. 15, no. 2, pp. 63–86, Feb. 2024, doi: https://doi.org/10.4236/jis.2024.152006

[57] K. AL-Dosari and N. Fetais, "Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach," *Electronics*, vol. 12, no. 17, p. 3629, Jan. 2023, doi: https://doi.org/10.3390/electronics12173629

[58] A. Efe, “A comparison of key risk management frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT,” *DenetimveGüvenceHizmetleriDergisi*, vol. 3, no. 2, pp. 185–205, Jul. 2023, Available: https://dergipark.org.tr/en/pub/audas/issue/79262/1291915

[59] J. Marquez-Tejon, Montserrat Jiménez Partearroyo, and D. Benito-Osorio, “Integrated security management model: a proposal applied to organisational resilience,” *Security Journal*, Jun. 2023, doi: https://doi.org/10.1057/s41284-023-00381-6

[60] A. AL-Hawamleh, “Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security,” *International Journal of Computing and Digital Systems*, vol. 15, no. 1, pp. 1315–1331, Mar. 2024, doi: https://doi.org/10.12785/ijcds/150193

[61] IBM, “Database Security: An Essential Guide | IBM,” *www.ibm.com*, 2023. https://www.ibm.com/topics/database-security

[62] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, “A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience,” *Sensors*, vol. 23, no. 16, p. 7273, Jan. 2023, doi: https://doi.org/10.3390/s23167273

Appendix

Sample size: 372

Section 1: Respondent Demographics

1. Your Role in the Organization:

- [ ] Executive
- [ ] Risk Management Specialist
- [ ] IT/Security Personnel
- [ ] Forensics Analyst
- [ ] Compliance Officer
- [ ] Other (Please Specify): _____

2. Organization's Industry:

- [ ] Financial Services
- [ ] Healthcare
- [ ] Technology
- [ ] Manufacturing
- [ ] Government
- [ ] Other (Please Specify): _____

3. Organization Size:

- [ ] Small (1-100 employees)
- [ ] Medium (101-500 employees)

- [ ] Large (>500 employees)

4. Years of Experience in Your Field:

- [ ] Less than 1 year
- [ ] 1-5 years
- [ ] 6-10 years
- [ ] More than 10 years

5. Age Group:

- [ ] Under 25
- [ ] 25-34
- [ ] 35-44
- [ ] 45-54
- [ ] 55-64
- [ ] 65 or older

6. Gender:

- [ ] Male
- [ ] Female
- [ ] Non-binary/Third gender
- [ ] Prefer not to say
- [ ] Other (Please Specify): _____

Section 2: Integration of ERM, ISO 27001, and Mobile Forensics

5. Current Implementation Status:

- [ ] Fully integrated ERM, ISO 27001, and mobile forensics
- [ ] Partially integrated
- [ ] Implemented independently, not integrated
- [ ] Not implemented

6. Reasons for Integration or Lack Thereof:

- [ ] Strategic decision to enhance digital security
- [ ] Compliance with legal or regulatory requirements
- [ ] Recommendations from security audits
- [ ] Lack of resources or expertise
- [ ] Other (Please Specify): _____

Section 3: Impact on Digital Risk Management

7. Ability to Identify Digital Risks:

- [ ] Significantly improved
- [ ] Somewhat improved
- [ ] No change
- [ ] Somewhat decreased
- [ ] Significantly decreased

8. Effectiveness in Assessing Digital Risks:

- [ ] Significantly more effective
- [ ] Somewhat more effective
- [ ] Unchanged
- [ ] Somewhat less effective
- [ ] Significantly less effective

9. Mitigation of Digital Risks:

- [ ] Highly effective
- [ ] Moderately effective
- [ ] Slightly effective
- [ ] Not effective

Section 4: Improvement in Information Security Management Practices

10. Compliance with Information Security Standards:

- [ ] Greatly enhanced
- [ ] Somewhat enhanced
- [ ] No significant change
- [ ] Somewhat diminished
- [ ] Greatly diminished

11. Data Protection Measures:

- [ ] Significantly improved
- [ ] Somewhat improved
- [ ] No significant change
- [ ] Somewhat worsened
- [ ] Significantly worsened

12. Incident Response Efficiency:

- [ ] Much faster
- [ ] Somewhat faster
- [ ] Unchanged
- [ ] Somewhat slower
- [ ] Much slower

Section 5: Enhancements in Digital Crime Investigation

13. Effectiveness of Mobile Forensics Investigations

- [ ] Significantly more effective
- [ ] Somewhat more effective
- [ ] Unchanged
- [ ] Less effective

14. Efficiency of Digital Crime Investigation Processes

- [ ] Much more efficient
- [ ] Somewhat more efficient
- [ ] Unchanged
- [ ] Less efficient