Journal of Business and Management Studies
ISSN: 2709-0876
DOI: 10.32996/jbms
Journal Homepage: www.al-kindipublisher.com/index.php/jbms

JBMS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Risk Governance Ecosystem in Information Communications Technology Industry using the Three Lines of Defense (3LOD) Framework Approach in the Philippines

Carlwin A. Mozar[1], **Antonio Errol B. Ybañez**[2] **and Emmanuel P. Paulino**[3] ✉

[1]DBA, De La Salle University Dasmarinas, College of Business Administration
[2]Jr., DBA, De La Salle University Dasmarinas, College of Business Administration
[3]DBA, LPT, Associate Professor, De La Salle University Dasmarinas, College of Business Administration

Corresponding Author: Emmanuel P. Paulino, **E-mail**: eppaulino@dlsud.edu.ph

| ABSTRACT

Several frameworks have been developed to ensure organizational compliance and resilience amid the increasing complexity of risks in the Information and Communication Technology (ICT) industry. This study explores the risk governance ecosystem of the Philippine ICT sector through the lens of the Three Lines of Defense (3LOD) framework, which comprises operational management, risk oversight, and independent assurance. These components are known for offering a structured approach to risk management and internal control. Using a quantitative research design, data were collected from 225 ICT professionals in the National Capital Region (NCR), including compliance officers, risk managers, financial executives, and internal auditors. The study examined the extent to which risk culture, regulatory environment, and ICT infrastructure influence the implementation of the 3LOD framework. Descriptive findings revealed that all three predictors were perceived to have a "very high effect," with ICT infrastructure ($\bar{x}$ = 3.53) ranking highest in its perceived influence. However, inferential analysis showed that ICT infrastructure had the most significant effect across all 3LOD components operation management (β = 0.4861, p = 0.003), risk management and compliance (β = 0.6449, p < .001), and internal audit (β = 0.7715, p < .001). Regulatory environment had a significant impact on operation management (β = 0.4007, p < .001), but its influence on risk and audit functions was statistically non-significant. Despite being rated highly, risk culture exhibited no significant effect on any governance components, suggesting a gap between cultural awareness and operational integration. The study contributes theoretically by reinforcing socio-technical systems theory, emphasizing that technological systems are foundational to risk governance. It challenges traditional views that prioritize risk culture without operational mechanisms and partially validates institutional theory by showing that regulatory influence is more apparent in external-facing functions. The proposed framework highlights ICT infrastructure as the central enabler, regulatory environment as a partial driver, and risk culture as an underutilized foundational element. Ultimately, this research offers empirical support for enhancing the 3LOD framework's implementation in the ICT industry. It provides insights for refining governance strategies, informing policy formulation, and guiding future research across diverse ICT environments to promote more resilient and adaptive risk management practices in the Philippines.

| KEYWORDS

Risk Culture, Regulatory Environment, ICT Infrastructure, 3LOD Framework

| ARTICLE INFORMATION

ACCEPTED: 01 August 2025 **PUBLISHED:** 14 September 2025 **DOI:** 10.32996/jbms.2025.7.5.10

1. Introduction

The rapid development of the Information and Communication Technology (ICT) industry has brought about transformative changes in economies worldwide, with the Philippines being no exception. The industry has become a critical enabler of digital innovation, economic growth, and the adoption of new technologies (Kim, Torneo, & Yang, 2019; Sarangi & Pradhan, 2020). However, as the ICT landscape evolves, so too does the complexity of the risks associate with it. To effectively manage these risks, it is crucial to develop comprehensive governance models that address the unique challenges posed by this dynamic environment (Birkel et al., 2019).

Risk governance in the ICT industry is particularly significant in the context of regulatory pressures, cybersecurity challenges, and the need for sustainable growth (Hernandez & Ona, 2019; Freitag et al., 2021). One promising framework for achieving effective risk governance is the Three Lines of Defense (3LOD) framework, which provides a structured approach to identifying, managing, and mitigating risks within organizations (Hu & Denizkurdu, 2020). The 3LOD framework emphasizes the roles of operational management, risk management, and internal audit in safeguarding organizational objectives and ensuring compliance with external regulations (Vaughan, 2022).

In the Philippines, the ICT industry faces unique challenges, including regulatory gaps, varying levels of infrastructure development, and a complex risk culture that must be carefully navigated (Cruz, Ting, & Tenido, 2021; Adam, Alhassan, & Afriyie, 2020). These challenges are compounded by the rapid pace of technological change, which demands that risk governance framework be flexible and adaptive to new risks and emerging threats (Milić, Borocki, & Vekić, 2024). Thus, there is an urgent need to develop a tailored risk governance ecosystem that integrates the 3LOD framework to enhance the effectiveness of risk management practices in the Philippine ICT industry.

This study proposes a framework for risk governance in the ICT industry of the Philippines using the 3LOD framework. The framework aims to address the industry's specific needs by providing a structured approach to risk identification, assessment, and mitigation while considering the complexities of the regulatory environment and evolving ICT infrastructure. By examining the interrelationship between the three lines of defense, this research seeks to contribute to the development of a robust risk governance ecosystem that can support the sustainable growth and resilience of the Philippine ICT industry (Kumari & Singh, 2024; Seidenfuss, Young, & Datwani, 2023).

Through this study, we aim to provide insights into the application of the 3LOD framework in the context of the ICT sector, addressing the existing gaps in risk management and governance practices while contributing to the ongoing discourse on effective risk governance models in emerging markets like the Philippines.

2. Risk Culture

Birkel et al. (2019) demonstrate that Industry 4.0 demands adaptive risk frameworks that align technological transformation with sustainability, a view that connects with Niyafard et al. (2024), who highlight how information technology mediates management skills and risk management to improve project outcomes in construction. Both studies emphasize the critical role of technology in embedding resilience and sustainability into organizational risk strategies. Kumar and Anbanandam (2020) extend this logic by showing that a strong risk culture within manufacturing enhances supply chain resilience, while Chen et al. (2021) underscore that risk awareness in finance underpins digital economic growth. Together, these works position culture and awareness as enablers of sustainable, technology-driven risk management.

Cultural influences on risk are further evidenced by Huang, Ma, and Wang (2022), who show how clan culture shapes organizational risk-taking, and Kucharska (2021), who finds that mistake acceptance fosters tacit knowledge sharing and innovation. Both point to culture as a driver of learning and adaptation, aligning with Saeidi et al. (2019), who argue that enterprise risk management (ERM) integrated with IT enhances competitive advantage. Complementing these perspectives, Olaniyi and Omubo (2023) stress that compliance with structured frameworks such as COSO strengthens IT auditing, governance, and sustainability, reinforcing the role of standards in guiding cultural practices.

Leadership further anchors risk culture. Tone (2018) and IRM (2020) emphasize that top management shapes employee attitudes and perceptions of risk, while Garcia (2020) and Cruz (2021) highlight the importance of Philippine ICT leaders balancing innovation with cyber risk reduction. Minter (2019) adds that leadership commitment strengthens compliance and operational resilience, illustrating how leaders act as catalysts for embedding robust risk cultures across industries.

Transparency complements leadership in sustaining trust and accountability. Aven (2016) and IAPP (2022) show that open communication of risk exposures and mitigation strategies fosters stakeholder confidence, a point reinforced by Avgerou (2020) in the context of data privacy. In the Philippines, compliance with the Data Privacy Act of 2012 (National Privacy Commission, 2020) makes transparency a necessity, while Cruz (2021) notes that open governance systems enhance accountability. Similarly, Aguilera and Cuervo-Cazurra (2020) and Bowen and Ostroff (2021) argue that transparency strengthens coordination across departments and aligns risk management with corporate goals.

Standards provide the structural backbone for these cultural and leadership practices. ISO (2018), Aven (2016), and NIST (2018) highlight that established frameworks such as ISO 31000 and the NIST Cybersecurity Framework create common vocabularies and uniform procedures. The DICT (2022) has promoted global standards in the Philippine ICT sector, helping firms align with international practices. EY Global (2021) and Cruz (2021) note that adherence to standards enables organizations to anticipate emerging risks such as cyberattacks while ensuring compliance and consistency.

Collectively, these studies demonstrate that risk management effectiveness is shaped by the interplay of technology, culture, leadership, transparency, and standards. Technology and IT integration enhance agility and resilience (Birkel et al., 2019; Niyafard et al., 2024; Saeidi et al., 2019), culture and leadership embed risk awareness and innovation (Kumar & Anbanandam, 2020; Kucharska, 2021; Tone, 2018; Garcia, 2020), transparency fosters accountability and trust (Aven, 2016; IAPP, 2022; Cruz, 2021), and standards ensure regulatory alignment and consistency (ISO, 2018; DICT, 2022; Olaniyi & Omubo, 2023). Together, they present a holistic view: effective risk governance in ICT and related industries requires not just technical solutions but also cultural reinforcement, ethical leadership, transparent governance, and global standards.

3. Regulatory Environment

Adam, Alhassan, and Afriyie (2020) establish that supportive regulatory frameworks drive the growth of global e-commerce by ensuring secure transactions, consumer protection, and fair competition. This role of regulation as an enabler of innovation and growth is echoed by Park and Choi (2019), who show that national-level digital innovation and economic transformation are accelerated by policies that provide stability and support for technology adoption. Isabelle et al. (2020) extend this logic through Porter's Five Forces, emphasizing how regulatory forces shape industry dynamics, influencing competition, barriers to entry, and strategic decision-making. Together, these studies highlight regulation as a determinant of both technological diffusion and competitive behavior.

In sustainability contexts, Hao, Guo, and Wu (2022) demonstrate that stringent environmental regulations, when combined with ICT, improve energy efficiency and green practices, complementing Freitag et al. (2021), who review ICT's climate impact and call for stronger policies to mitigate its footprint. Antoni, Jie, and Abareshi (2020) reinforce this by showing that regulatory support drives Indonesian ICT firms to adopt eco-friendly practices, while Song, Wang, and Zhang (2020) argue that environmental regulations paired with R&D incentives stimulate green product innovation. Collectively, these studies illustrate that environmental regulation not only mitigates harm but also creates opportunities for technological and product innovation.

These global insights parallel the Philippine context, where environmental laws such as the Ecological Solid Waste Management Act (RA 9003) and the Clean Air Act (RA 8749) are central to regulating ICT's environmental toll (Cruz, 2021; DENR, 2020; SWMC, 2019). Such policies reflect Freitag et al.'s (2021) call for strong regulation, emphasizing waste management, carbon reduction, and green technology promotion.

Cybersecurity laws provide another dimension of regulatory impact. Cabral (2022) notes that digitalization has heightened the urgency for robust legislation, with the Cybercrime Prevention Act of 2012 (RA 10175) and the Data Privacy Act of 2012 serving as the foundation for ICT security. However, UNCTAD (2022) and DIT (2023) caution that enforcement and coordination between public and private entities remain weak, requiring updates to counter evolving threats like ransomware and cyber espionage. This aligns with Adam et al. (2020), who highlight regulation's role in protecting trust in digital commerce, showing that without strong cybersecurity, e-commerce growth is undermined.

Data privacy regulations also underpin digital trust. Reyes (2022) stresses their growing importance as personal data use expands, while the NPC (2021) acknowledges compliance progress yet notes gaps in awareness and implementation, particularly among SMEs. Kabigting (2023) further emphasizes the need for training to strengthen organizational capacity for compliance. These findings connect to Isabelle et al. (2020) and Park and Choi (2019), as privacy laws not only safeguard individuals but also enable sustained digital innovation by building consumer confidence.

Collectively, these studies reveal a consistent pattern: regulatory frameworks across domains e-commerce, environmental sustainability, cybersecurity, and data privacy shape technological adoption, risk management, and competitive advantage. Global evidence (Adam et al., 2020; Hao et al., 2022; Freitag et al., 2021; Song et al., 2020) aligns with Philippine-specific laws (Cruz, 2021; Cabral, 2022; Reyes, 2022), underscoring that effective regulation not only ensures compliance but also fosters innovation, strengthens resilience, and supports sustainable growth in ICT and beyond.

4. ICT Infrastructure

Sarangi and Pradhan (2020) highlight the role of ICT infrastructure as a catalyst for productivity and efficiency, particularly in developing economies, which resonates with Milić, Borocki, and Vekić (2024), who emphasize ICT's contribution to innovation ecosystems and business competitiveness. Adeola and Evans (2020) extend this perspective by demonstrating how ICT infrastructure enhances tourism in Africa through improved communication and service delivery, while Azolibe and Okonkwo (2020) confirm its pivotal role in boosting industrial productivity and diversification in Sub-Saharan Africa. These findings are reinforced by Heo and Lee (2019), who show how ICT infrastructure serves as a central node in Korea's economic networks, influencing value chains across multiple sectors. Similarly, Kurniawati (2020) and Kumari and Singh (2024) reveal that ICT infrastructure, when combined with globalization and financial development, significantly drives economic growth, though with stronger effects in high-income countries with mature institutional frameworks.

Beyond growth, ICT infrastructure has been linked to sustainability outcomes. Hao, Guo, and Wu (2022) demonstrate that environmental regulations, when paired with advanced ICT, improve energy efficiency, while Freitag et al. (2021) emphasize the need for regulatory measures to reduce ICT's environmental footprint. Sun and Kim (2021) add that ICT supports green practices and lowers carbon intensity, showing that digitalization and sustainability can progress together. Antoni, Jie, and Abareshi (2020) reinforce this by showing that regulatory support encourages firms to adopt eco-friendly ICT practices, while Song, Wang, and Zhang (2020) demonstrate how environmental regulations and tax incentives stimulate green product innovation. Together, these studies illustrate that ICT infrastructure, when supported by effective regulation, can simultaneously promote growth, innovation, and environmental stewardship.

These global insights connect to the Philippine context, where the IT ecosystem is expanding through initiatives like "Digital Philippines" (DICT, 2021), backed by domestic and foreign investment (USAID, 2020; ADB, 2020; OECD, 2020). The country's thriving BPO industry (Frost & Sullivan, 2020; ITA, 2020) and growing innovation networks underscore the importance of ICT infrastructure as a backbone for economic and social transformation. Data centers are emerging as a critical component, with rising investment driven by demand for cloud services and digital transactions (AWS, 2022; Globe Telecom, 2022), though challenges remain in sustainability, power reliability, and connectivity (Global Data, 2021; IFC, 2021). Internet connectivity further illustrates these gaps: despite over 76 million internet users by 2022, the Philippines lags in broadband speed (Ookla, 2023), highlighting the urgency of programs such as the National Broadband Program (DICT, 2022) and the need for public-private partnerships to accelerate infrastructure development (ADB, 2022; World Bank, 2021).

Collectively, these studies show that ICT infrastructure plays a multi-dimensional role in economic growth, innovation, industrial productivity, tourism development, and environmental sustainability. However, its transformative potential depends on continuous investment, regulatory support, and strategies to address barriers such as cybersecurity risks (Peraković et al., 2019), connectivity gaps, and infrastructural weaknesses. For the Philippines, strengthening ICT infrastructure through robust ecosystems, sustainable data centers, and improved internet connectivity is essential not only for competitiveness but also for fostering inclusive and sustainable digital transformation.

5. 3LOD Framework

The Three Lines of Defense (3LOD) framework has emerged as a foundational model for risk management and governance, but scholars continue to debate its adaptability to modern organizational realities. Seidenfuss, Young, and Datwani (2023) argue that integrating governance, risk, and compliance (GRC) within the updated framework enhances synergy and flexibility, a point that complements Kahler's (2020) findings on the need to redefine roles such as internal audit and Data Protection Officers to meet evolving regulatory requirements. Similarly, Hu and Denizkurdu (2020) challenge traditional self-assessment approaches, stressing proactive risk identification, while Vaughan (2022) and Borg et al. (2020) critique the framework's rigidity in financial contexts, arguing for more dynamic and responsive applications to address emerging risks like financial crime and cybersecurity. Turner (2022) echoes this critique, warning that the framework's structured but inflexible design may not suit fast-changing environments. Collectively, these perspectives suggest that while the 3LOD framework remains central to organizational oversight, its continued relevance depends on its ability to adapt to regulatory shifts and complex risk landscapes.

At the operational level, scholars emphasize the importance of the first line of defense in embedding risk considerations into daily activities. Pavlou and El Sawy (2010) underscore the need for ICT firms in emerging economies to align operations with risk tolerance to sustain service quality and resilience. Van der Merwe and Van Dyk (2020) extend this by highlighting the responsibility of operations to identify risks from new technologies such as cloud computing and artificial intelligence. Zhao et al. (2018) reinforce that cultivating a risk-aware culture and investing in training strengthens operational continuity, while Tuano and Quimbo (2021) note that Philippine ICT firms face unique barriers, such as regulatory lag and infrastructure gaps, necessitating stronger internal capabilities to manage risks effectively.

The second line of defense, focused on compliance and risk management, ensures that operational practices align with regulatory requirements. Bhimani (2021) emphasizes that ICT risk management strategies are effective only when compliance mechanisms integrate both local and international standards. This is particularly relevant in the Philippines, where Martinez and Diaz (2020) highlight the pressures of aligning with the Data Privacy Act and the National Cybersecurity Plan. Deloach and Andersen (2017) further stress that embedding risk management activities within the 3LOD is essential for managing data breaches and cybersecurity threats, while Regoniel (2022) underscores the dual responsibility of compliance functions to enforce current laws and anticipate risks stemming from future technological and regulatory changes.

Finally, the third line of defense internal audit serves as the assurance mechanism that validates the effectiveness of both operational and compliance functions. The Institute of Internal Auditors reports that ICT audits increasingly focus on cybersecurity and data governance, a trend echoed by Lopez and Domingo (2021), who show that IT audits in the Philippines now complement financial audits in scope. KPMG (2019) and PwC (2021) highlight the global role of internal audit in ensuring adherence to cybersecurity and data protection standards while also evaluating risk systems' capacity to adapt to digital transformation. Collectively, these findings underscore that internal audit is no longer limited to financial assurance but plays a strategic role in validating ICT firms' risk governance in a rapidly evolving digital environment.

Together, these strands of literature suggest that while the 3LOD framework remains a cornerstone of risk governance, its effectiveness depends on continuous adaptation. At the governance level, its flexibility must be enhanced to address emerging risks and regulatory complexity; at the operational level, firms must strengthen their cultures and systems to manage technological disruptions; at the compliance level, alignment with both local and global standards is vital; and at the audit level, expanding scope into ICT and digital transformation risks ensures resilience. The coherence of these functions demonstrates that the 3LOD is not static but an evolving model that requires integration, cultural reinforcement, and regulatory alignment to remain effective in contemporary risk environments.

6. Risk Culture Linked with 3LOD Framework

Grebe and Marx (2023) demonstrate that strong leadership commitment, ethical standards, and risk awareness in Ghanaian banks foster better alignment with the Three Lines of Defense (3LOD) framework, a finding echoed by Molelekoa (2022), who shows that embedded risk culture strengthens coordination and accountability among the lines. Extending this perspective, Patipan (2024) highlights how data-driven tools, such as text analytics, can reveal gaps in risk communication, offering organizations a practical way to reinforce cultural alignment across the 3LOD. Similarly, Park (2019) finds that bureaucratic barriers in the Australian public sector hinder 3LOD implementation, but that encouraging open risk dialogue improves governance outcomes an argument consistent with Bertin (2024), who stresses the importance of cultivating risk-aware cultures in non-profit settings with limited oversight resources.

These insights converge with Hoefer, Cooke, and Curry (2020), who argue that the 3LOD often fails where compliance is emphasized over genuine risk understanding, calling for continuous cultural transformation and education to close these gaps. Supporting this, Kheswa (2023) shows that banks with robust risk cultures achieve stronger, more transparent risk reporting, thereby enabling the 3LOD to function effectively. Taken together, these studies illustrate a symbiotic relationship: a strong risk culture promotes accountability, awareness, and communication across all three lines, while weak or compliance-driven cultures undermine the integrity of the framework and expose organizations to governance failures.

H_a1: There is no significant effect of risk culture on operation management.
H_a2: There is no significant effect of risk culture on risk management and compliance.
H_a3: There is no significant effect of risk culture on internal audit.

6.2 Regulatory Environment Linked with 3LOD Framework

Pecina, Sprčić, and Lacković (2022) show that regulatory requirements in the European power sector strengthen the Three Lines of Defense (3LOD) framework by improving coordination across operational, risk, and audit functions. This aligns with Pantos (2024) and Genovesi (2025), who stress that evolving AI regulations, such as the UK prudential framework and the EU AI Act, require flexibility in the second and third lines to address emerging risks. Jauhiainen and Lehner (2022) add that regulatory gaps in AI and big data weaken 3LOD effectiveness, reinforcing the need for stronger oversight functions. Similarly, Migliorelli and Marini (2020) argue that ESG disclosure requirements embed sustainability risks into governance, strengthening the second line's monitoring role and the third line's assurance function.

Balancing these benefits, Butler and Brooks (2023) warn that compliance-heavy approaches may foster box-ticking rather than genuine risk mitigation. Their critique contrasts with Zeier Röschmann et al. (2019), who show that Swiss insurers adapt to complex regulatory demands through clearer roles, stronger communication, and alignment with standards.

Taken together, these studies confirm that regulation is both a catalyst and a challenge for effective 3LOD implementation. On one hand, evolving regulatory frameworks whether in traditional industries (Pecina et al., 2022; Zeier Röschmann et al., 2019), AI governance (Pantos, 2024; Genovesi, 2025; Jauhiainen & Lehner, 2022), or sustainability reporting (Migliorelli & Marini, 2020) expand the scope and accountability of the second and third lines of defense. On the other hand, as Butler and Brooks (2023) warn, organizations must balance compliance with proactive risk mitigation to avoid complacency. The overarching implication is that highly regulated environments necessitate flexible, adaptive, and balanced applications of the 3LOD framework in order to maintain resilience and credibility in governance systems.

H_a4: There is a significant effect of regulatory environment on operation management.
H_a5: There is no significant effect of regulatory environment on risk management and compliance.
H_a6: There is no significant effect of regulatory environment on internal audit.

6.3 ICT Infrastructure Linked with 3LOD Framework

Turk et al. (2022) emphasize that cybersecurity embedded within ICT infrastructure safeguards operational systems and data, directly supporting the first line of defense by reducing vulnerabilities that could disrupt organizational operations. This argument connects with Novaes Neto et al. (2020), who illustrate through the Capital One breach that weaknesses in cybersecurity not only compromise day-to-day operations but also expose the need for oversight mechanisms from the second line of defense. Together, these studies demonstrate how operational management and risk management are interdependent: operations must adopt strong security protocols, while risk managers ensure that these measures are properly implemented and maintained.

Building on this, Walter and Narring (2020) highlight how ICT infrastructure further strengthens the second line of defense by embedding transparency and governance principles into risk management practices. Their focus on governance resonates with Wall (2021), who shows that AI-driven compliance systems enhance both the first and second lines by automating monitoring and ensuring that governance standards are consistently applied in real time. In this way, Walter and Narring's emphasis on ethical oversight is operationalized by Wall's evidence of AI systems, which provide the tools needed to enforce compliance and minimize risks across multiple lines of defense.

Extending this discussion, Tammenga (2020) demonstrates that artificial intelligence also transforms the third line of defense by strengthening internal audit functions in the banking sector. AI technologies enable real-time monitoring and anomaly detection, which complements the governance and compliance mechanisms discussed by Walter and Narring (2020) and Wall (2021). When placed in context, Tammenga's findings illustrate how advanced ICT tools not only monitor compliance but also ensure that audits provide independent and continuous verification of operational and risk management practices.

Taken together, these studies show that ICT infrastructure underpins the entire Three Lines of Defense (3LOD) framework by integrating cybersecurity and AI technologies across all organizational levels. Cybersecurity ensures resilience in operations (Turk et al., 2022; Novaes Neto et al., 2020), governance and compliance frameworks strengthen transparency and oversight (Walter & Narring, 2020; Wall, 2021), and AI-enabled auditing provides independent assurance (Tammenga, 2020). Collectively, this body of work underscores that ICT infrastructure is not merely technical support but a strategic enabler of risk governance, linking operational reliability, risk oversight, and internal assurance into a coherent system.

H_a7: There is a significant effect of ICT infrastructure on operation management.
H_a8: There is a significant effect of ICT infrastructure on risk management and compliance.
H_a9: There is a significant effect of ICT infrastructure on internal audit.

7. Conceptual Framework of the Study

Figure 1 presents the structured representation that explains the relationships among key variables.

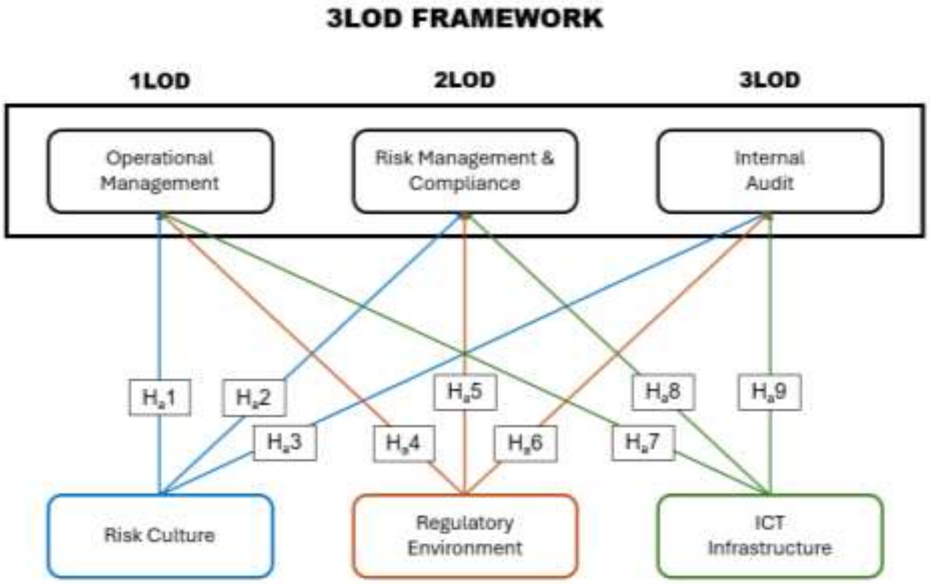

Figure 1. Conceptual Framework of the Study

This study's conceptual framework examines how risk culture, the regulatory environment, and ICT infrastructure influence the Three Lines of Defense (3LOD) framework in the Philippine ICT industry. Risk culture shapes proactive risk identification and mitigation, while regulations establish compliance obligations, and ICT infrastructure provides the technological foundation for effective operations and risk governance. Within the 3LOD model, operational management directly handles risks, risk management and compliance ensure oversight, and internal audit provides independent evaluation. Together, these elements strengthen organizational risk governance, enabling firms to address risks, maintain regulatory compliance, and sustain efficient operations.

8. Methodology

8.1 Population and Sampling

This study was conducted in the Information and Communication Technology (ICT) industry within the National Capital Region (NCR), also known as Metro Manila. As the country's political and economic hub, NCR hosts the largest and most diverse concentration of ICT firms, ranging from multinational corporations to small and medium-sized enterprises. These companies provide a wide array of services, including customer support, technical assistance, back-office operations, and various IT solutions, making NCR the most strategic site for examining risk governance and employee engagement.

Participating firms included leading industry players such as IBM Philippines, Cisco Systems Philippines, Accenture Philippines, PLDT Group, Globe Telecom, and Eastern Communications, among others. The inclusion of companies with different sizes, service portfolios, and organizational cultures ensured that the findings would be broadly applicable across the ICT sector. While the industry offers substantial opportunities for risk governance practices, challenges such as role clarity, training needs, and resistance to change in some organizations can affect the effective implementation of the Three Lines of Defense (3LOD) framework.

Despite these challenges, ICT firms in NCR that foster strong risk management cultures and remain committed to refining their governance frameworks tend to achieve better outcomes in terms of risk mitigation and organizational performance. Thus, NCR provides an ideal setting for this research, offering valuable insights into how risk governance structures can strengthen employee engagement and contribute to sustained competitiveness in the Philippine ICT industry.

8.2 Instrumentation and Data Gathering

The researcher formally reached out to qualified ICT firms through letters requesting participation in the study. From these, randomly selected firms were invited to allow the administration of surveys and interviews for data collection. Upon receiving approval, the participating firms were provided with a Google Forms link to complete the survey. Responses were recorded in spreadsheets (Microsoft Excel or Google Sheets), which served as the primary basis for analysis. All data were handled with strict adherence to privacy and confidentiality protocols to ensure that only relevant information was collected and properly evaluated.

Data were gathered using a self-developed survey questionnaire designed to measure the key variables of the study. Each item in the questionnaire was aligned with the constructs under investigation and measured using a four-point Likert scale with the following descriptors: 1 – No Effect, 2 – Very Low Effect, 3 – High Effect, and 4 – Very High Effect.

Descriptive statistics were used to summarize the profile of participating ICT firms and to evaluate the extent of Risk Culture, Regulatory Environment, ICT Infrastructure, and the Three Lines of Defense (3LOD) constructs. Frequencies were generated to describe firm characteristics, while means and standard deviations were computed to assess the overall level of each construct. The four-point Likert scale (1 = No Effect, 4 = Very High Effect) provided the basis for interpreting responses. Partial Least Squares Structural Equation Modeling (PLS-SEM) was then employed to examine the hypothesized relationships among the constructs.

Table 1. Interpretation of Scores and Mean Values

Range of Mean Values	Weight	Interpretation
3.26 – 4.00	4	Very High Effect
2.51 – 3.25	3	High Effect
1.75 – 2.50	2	Very low Effect
1.00 – 1.74	1	No Effect

Descriptive statistics were utilized to summarize the survey responses of construction service firms in the study. Percentage tables were employed to describe the distribution of participating firms, while arithmetic means were computed to assess the scale measurements derived from the questionnaire. The arithmetic mean, which gives equal weight to all numerical responses, was applied to avoid bias in the analysis of the survey data.

Partial Least Squares Structural Equation Modeling (PLS-SEM) was applied to examine the complex relationships among Risk Culture, Regulatory Environment, ICT Infrastructure, and the constructs of the Three Lines of Defense (3LOD), namely Operation Management, Risk Management and Compliance, and Internal Audit, in the ICT industry of the Philippines. PLS-SEM was chosen because it is a variance-based approach well-suited for exploratory and predictive research, particularly when handling complex models and relatively small sample sizes. This method enables the simultaneous evaluation of the measurement model, which assesses the reliability and validity of questionnaire items in capturing their intended constructs, and the structural model, which evaluates the hypothesized relationships among constructs.

In this study, PLS-SEM facilitated the testing of direct and indirect effects to determine how organizational factors influence the successful implementation of the 3LOD framework in the ICT sector. All analyses were performed using WarpPLS statistical software, ensuring rigorous assessment of both measurement and structural components of the model.

9. Results and Discussion

9.1 Data Analysis

Table 2 Construct Validity and Scale Reliability

Construct	Items	Loadings	Ave. Var. Ext.	Cronbach's a
Leadership	1	0.69	0.91	0.59
	2	0.74		
	3	0.73		
	4	0.84		
	5	0.83		
Transparency	4	0.70	0.94	0.543
	2	0.77		
	5	0.69		
	3	0.73		
	1	0.79		
Standard	5	0.72	0.85	0.604
	1	0.82		
	3	0.80		
	4	0.73		
	2	0.81		
Environmental Regulations	5	0.68	0.93	0.591
	1	0.86		
	2	0.83		
	3	0.75		
	4	0.71		
Cybersecurity Laws	3	0.75	0.95	0.591
	4	0.70		
	4	0.70		
	1	0.87		
	2	0.81		
Data Privacy Regulations	2	0.84	0.93	0.671
	3	0.80		
	1	0.89		
	4	0.76		
	3	0.80		
IT Ecosystem	3	0.82	0.93	0.653
	1	0.87		

	4	0.81		
	2	0.84		
	5	0.69		
Data Centers	1	0.74	0.87	0.522
	4	0.70		
	3	0.73		
	4	0.70		
	1	0.74		
Internet Connectivity	2	0.76	0.91	0.606
	2	0.76		
	5	0.73		
	4	0.74		
	1	0.89		
Operation Management	2	0.81	0.91	0.595
	4	0.72		
	1	0.84		
	4	0.72		
	3	0.76		
Risk Management & Compliance	4	0.82	0.95	0.696
	5	0.80		
	3	0.83		
	1	0.87		
	2	0.85		
Internal Audit	5	0.69	0.87	0.582
	2	0.75		
	3	0.74		
	4	0.73		
	1	0.89		

Note: Cronbach's alpha should be larger than 0.70 for reliability. All loadings must be more than or equal to 0.50 for convergence validity, and all Average Variance Extracted should be => 0.50 when extracted.

All items in the questionnaire showed strong internal consistency, with composite reliability values above 0.70 and Cronbach's alpha coefficients also exceeding the 0.70 benchmark.

For validity, each item recorded factor loadings higher than 0.50, and the Average Variance Extracted (AVE) values were above the 0.50 cutoff. Together, these results confirm that the constructs are both reliable and valid, establishing their convergent validity.

9.2 Structural Model Evaluation

Structural Path Results

Table 3 Path Evaluation Results

Path Estimates					
Predictor	**Dependent**	**Estimate**	**SE**	**t**	**p**
Risk Culture	Operation Management	0.0988	0.114	0.869	0.385
Risk Culture	Risk Management and Compliance	0.196	0.128	1.538	0.124
Risk Culture	Internal Audit	0.0791	0.131	0.605	0.545
Regulatory Environment	Operation Management	0.4007	0.121	3.306	< .001
Regulatory Environment	Risk Management and Compliance	0.1249	0.141	0.886	0.376
Regulatory Environment	Internal Audit	0.118	0.138	0.858	0.391
ICT Infrastructure	Operation Management	0.4861	0.162	3.008	0.003
ICT Infrastructure	Risk Management and Compliance	0.6449	0.127	5.087	< .001
ICT Infrastructure	Internal Audit	0.7715	0.165	4.668	< .001

Note: If the p-value is lower than 5% or 0.05, it is statistically Significant. If the p-value is greater than 5%, the result is statistically non-significant.

Table 3 presents the results of the path evaluation for the hypothesized relationships among Risk Culture, Regulatory Environment, and ICT Infrastructure with Operation Management, Risk Management and Compliance, and Internal Audit. The effect of Risk Culture on Operation Management (Ha1) is positive but not statistically significant, with β = 0.0988, SE = 0.114, t = 0.869, and p = 0.385, indicating that Risk Culture does not directly influence operational outcomes. Similarly, its effect on Risk Management and Compliance (Ha2) is also not significant (β = 0.196, SE = 0.128, t = 1.538, p = 0.124), as well as its effect on Internal Audit (Ha3) (β = 0.0791, SE = 0.131, t = 0.605, p = 0.545), suggesting that Risk Culture does not exert a meaningful impact on these areas.

On the other hand, the Regulatory Environment demonstrates a significant positive influence on Operation Management (Ha4), with β = 0.4007, SE = 0.121, t = 3.306, and p < 0.001, thereby supporting the hypothesis that stronger regulatory conditions enhance operational processes. However, its effect on Risk Management and Compliance (Ha5) (β = 0.1249, SE = 0.141, t = 0.886, p = 0.376) and Internal Audit (Ha6) (β = 0.118, SE = 0.138, t = 0.858, p = 0.391) are both non-significant, indicating no substantial direct influence.

Lastly, ICT Infrastructure is shown to have consistently strong and significant effects across all three dependent variables. It significantly enhances Operation Management (Ha7) with β = 0.4861, SE = 0.162, t = 3.008, p = 0.003, Risk Management and Compliance (Ha8) with β = 0.6449, SE = 0.127, t = 5.087, p < 0.001, and Internal Audit (Ha9) with β = 0.7715, SE = 0.165, t = 4.668, p < 0.001. These findings highlight ICT Infrastructure as the most critical determinant in strengthening organizational systems, while Risk Culture shows no significant impact and the Regulatory Environment demonstrates a limited but noteworthy role in improving operations.

10. Conclusion

10.1 Risk Culture Linked with 3LOD Framework

Although risk culture was perceived to be strong, its statistical effect on operation management was found to be positive but not significant. This suggests that while risk-aware behaviors exist, they are not yet embedded deeply enough to significantly shape day-to-day operational activities.

Similarly, risk culture demonstrated a positive but statistically non-significant effect on risk management and compliance. This outcome suggests that there may be a gap between the organization's risk values and how these are practically implemented in compliance practices.

The effect of risk culture on internal audit was also statistically non-significant. Although internal audit functions benefit from a culture of risk awareness, the results indicate that this relationship has not yet been translated into a measurable influence, pointing to a need for better cultural integration in assurance activities.

10.2 Regulatory Environment Linked with 3LOD Framework

The regulatory environment had a significant and positive effect on operation management. This indicates that formal policies, compliance requirements, and regulatory oversight contribute meaningfully to the effectiveness and structure of operational activities in ICT firms.

The effect of the regulatory environment on risk management and compliance was found to be positive but statistically non-significant. This may suggest that while rules are in place, their operational impact within compliance processes is still limited or inconsistently enforced.

A similar pattern emerged for internal audit, where the regulatory environment had non-significant effect. This indicates potential misalignment between external regulation and internal audit structures, possibly due to resource constraints or gaps in institutional adaptation.

10.3 ICT Infrastructure Linked with 3LOD Framework

ICT infrastructure had a significant and positive effect on operation management. This confirms that technology plays a critical role in streamlining operations, enhancing efficiency, and supporting real-time decision-making across functions.
A highly significant and strong positive effect was found between ICT infrastructure and risk management and compliance. This finding confirms that digital tools and systems are central to enabling proactive risk monitoring, regulatory adherence, and compliance reporting.

ICT infrastructure was shown to have a strong and significant positive effect on internal audit. This highlights the growing importance of advanced digital systems in enabling more agile, data-driven, and continuous assurance practices within ICT organizations.

10.4 Implications

The findings of this study offer several theoretical contributions that help refine and contextualize existing frameworks in organizational governance and risk management. First, the significant influence of ICT infrastructure across all components of the 3LOD framework reinforces the socio-technical systems theory, which emphasizes the necessity of aligning technical systems such as infrastructure, platforms, and analytics organizational processes and controls to achieve effective governance. This observation aligns with the insights of Antoni et al. (2020) and ADB (2020), who highlighted that technology functions not merely as a tool but as a fundamental enabler of structured and strategic decision-making.

Second, while risk culture was rated very highly by respondents, it did not demonstrate any statistically significant effect on the governance components studied. This calls for a reassessment of how risk culture is integrated into formal governance models. The findings suggest a disconnect between espoused organizational values and actual practices, highlighting the need for risk culture to be institutionalized through mechanisms such as training, KPIs, and embedded procedures. In contrast to the assumptions of IRM (2020) and IIA (2020), this study suggests that culture alone without supportive systems may not be sufficient to influence governance outcomes.

Third, the results provide partial validation of institutional theory, particularly the notion of institutional isomorphism as proposed by DiMaggio and Powell. The regulatory environment was found to significantly influence only operational management, suggesting that institutional pressures such as laws and compliance mandates tend to shape externally visible practices. However, they may not deeply influence internal functions like risk compliance and audit systems, especially in organizations where enforcement levels and resource allocations vary.

Lastly, this study supports the expansion of the 3LOD governance framework, proposing that it be recalibrated to reflect the foundational role of ICT infrastructure. The evidence shows that technology is not simply a support mechanism but a central pillar for implementing effective risk governance. Furthermore, it underscores the importance of translating cultural values and regulatory principles into concrete, measurable practices. As such, the findings contribute to a more dynamic understanding of the 3LOD framework one that acknowledges the essential role of digital infrastructure while recognizing the limitations of culture and regulation in isolation.

10.5 Output of the Study

Figure 2 presents the estimated results of the hypothesized covariance structural model.

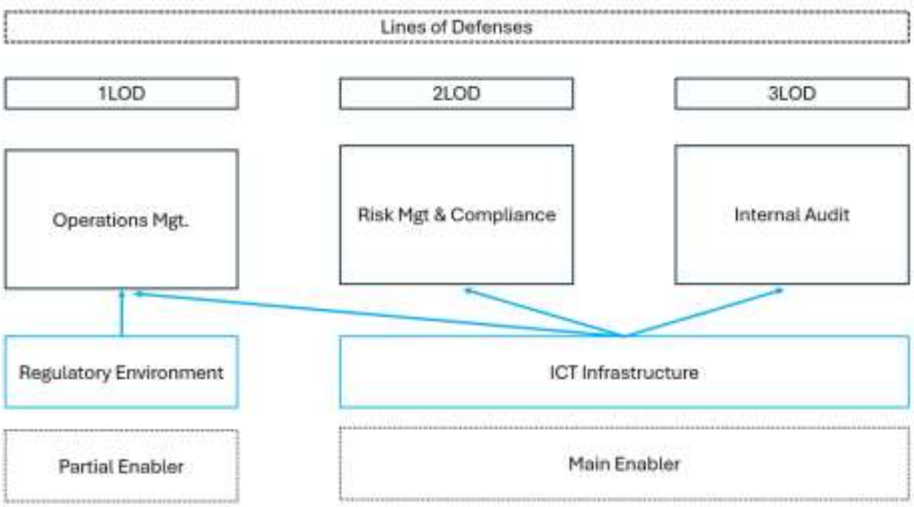

Figure 2. Path Evaluation Results Estimates

The Three Lines of Defense (3LOD) model serves as a widely recognized framework for governance, risk management, and internal control, and the diagram highlights the enabling roles of both the regulatory environment and information and communication technology (ICT) infrastructure within this structure. The first line of defense, operations management, is primarily responsible for directly managing risks in day-to-day organizational activities. The second line, risk management and compliance, provides oversight and establishes policies, standards, and monitoring systems to ensure that the first line effectively identifies and mitigates risks. The third line, internal audit, functions as an independent assurance mechanism, evaluating the adequacy and effectiveness of risk management, compliance, and control systems implemented by the first and second lines.

In this framework, the regulatory environment operates as a partial enabler by setting external compliance requirements and legal mandates that influence and shape operational practices, particularly within the first line of defense. ICT infrastructure, however, is positioned as the main enabler, providing the technological backbone that supports all three lines. For the first line, ICT enables operational efficiency and real-time monitoring of risks. For the second line, it enhances compliance oversight through automated reporting, analytics, and monitoring tools. For the third line, it facilitates independent, data-driven audits and continuous assurance processes. By enabling integration, transparency, and efficiency across all three lines, ICT infrastructure strengthens the organization's capacity to manage risks and ensures the reliability of governance mechanisms, thereby positioning itself as a critical foundation of the 3LOD model.

Funding: This research received no external funding
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers.

ORCID
Carlwin A. Mozar: ORCID ID: 0009-0009-5501-8244
Antonio Errol B. Ybañez: ORCID ID: https://orcid.org/0009-0004-9044-455X

Emmanuel P. Paulino: ORCID ID: https://orcid.org/0000-0002-6282-6460

References

[1] Adam, I. O., Alhassan, M. D., & Afriyie, Y. (2020). What drives global B2C E-commerce? An analysis of the effect of ICT access, human resource development and regulatory environment. *Technology Analysis & Strategic Management, 32*(7), 835-850. https://doi.org/10.1080/09537325.2020.1714579

[2] Adeola, O., & Evans, O. (2020). ICT, infrastructure, and tourism development in Africa. *Tourism Economics, 26*(1), 97-114. https://doi.org/10.1177/1354816619827712

[3] Aguilera, R. V., & Cuervo-Cazurra, A. (2020). "Codes of Good Governance." Corporate Governance: An International Review, 28(3), 208–224.

[4] Al-Kumaim, N. H., & Alshamsi, S. K. (2023). Determinants of cyberattack prevention in UAE financial organizations: assessing the mediating role of cybersecurity leadership. *Applied Sciences, 13*(10), 5839. https://doi.org/10.3390/app13105839

[5] Amazon Web Services (AWS). (2022). Expanding Cloud Infrastructure in Southeast Asia: The Role of Data Centers in the Philippines. AWS Industry Insights.

[6] Antoni, D., Jie, F., & Abareshi, A. (2020). Critical factors in information technology capability for enhancing firm's environmental performance: case of Indonesian ICT sector. *International Journal of Agile Systems and Management, 13*(2), 159-181. https://doi.org/10.1504/IJASM.2020.107907

[7] Asian Development Bank (ADB). (2020). "The Role of ICT in Enhancing Innovation in the Philippines." ADB Report.

[8] Aven, T. (2016). Risk Assessment and Risk Management: Review of Recent Advances on Their Foundation. *European Journal of Operational Research*.

[9] Avgerou, C. (2020). Transparency and Trust in ICT Governance: Global Standards and Corporate Practices. *Information Systems Journal*.

[10] Azolibe, C. B., & Okonkwo, J. J. (2020). Infrastructure development and industrial sector productivity in Sub-Saharan Africa. *Journal of Economics and Development, 22*(1), 91-109. https://doi.org/10.1108/JED-11-2019-0062

[11] Bertin, E. (2024). 2Implementing and maintaining an effective risk management system in non-profit organisations. Non-profit Governance: Twelve Frameworks for Organisations and Research. DOI: 10.4324/97810034605772

[12] Bertin, E. (2024). Implementing and maintaining an effective risk management system in non-profit organisations: A conceptual framework. In Non-profit Governance (pp. 29-47). Routledge. https://doi.org/10.4324/9781003460572

[13] Birkel, H. S., Veile, J. W., Müller, J. M., Hartmann, E., & Voigt, K. I. (2019). Development of a risk framework for Industry 4.0 in the context of sustainability for established manufacturers. Sustainability, 11(2), 384. https://doi.org/10.3390/su11020384

[14] Borg, G., Baldacchino, P. J., Buttigieg, S., Boztepe, E., & Grima, S. (2020). Challenging the adequacy of the Conventional 'Three lines of Defence'model: A case Study on Maltese Credit Institutions. In Contemporary issues in audit management and forensic accounting (Vol. 102, pp. 303-324). Emerald Publishing Limited. https://doi.org/10.1108/S1569-375920200000102021

[15] Bowen, H. P., & Ostroff, C. (2021). Understanding HRM-Firm Performance Linkages: The Role of the 'Strength' of the HRM System. *Academy of Management Review, 29*(2), 203–221.

[16] Butler, T., & Brooks, R. (2023). Time for a paradigm change: Problems with the financial industry's approach to operational risk. Risk Analysis. https://doi.org/10.1111/risa.14240

[17] Cabral, R. (2022). Addressing the Gaps in Cybersecurity Legislation: A Philippine Perspective. *Journal of Cybersecurity Policy*.

[18] Chen, Y., Kumara, E. K., & Sivakumar, V. (2021). Invesitigation of finance industry on risk awareness model and digital economic growth. *Annals of Operations Research*, 1-22. https://doi.org/10.1007/s10479-021-04287-7

[19] Cruz, C. E., Ting, K. A. I., & Tenido, P. I. D. (2021). Assessing IPR protection in the semiconductor and electronics industry in the Philippines: Challenges and opportunities in the global value chain. *Intellectual Property Rights and ASEAN Development in the Digital Age,* 114-143.

[20] Cruz, R. (2021). Challenges in Enforcing E-Waste Management Regulations in the Philippines. *Journal of Environmental Sustainability.*

[21] Deloitte. (2020). The Three Lines Model: Enhancing the Value of Risk Management. Deloitte Risk Advisory.

[22] Department of Environment and Natural Resources (DENR). (2020). Report on E-Waste Management in the Philippines. DENR Publications.

[23] EY Global. (2021). Cybersecurity Risk Management: Adapting to New Threats. Ernst & Young Insights.

[24] Freitag, C., Berners-Lee, M., Widdicks, K., Knowles, B., Blair, G., & Friday, A. (2021). The climate impact of ICT: A review of estimates, trends and regulations. arXiv preprint arXiv:2102.02622. https://doi.org/10.48550/arXiv.2102.02622

[25] Frost & Sullivan. (2020). The Growth of IT Services in the Philippines' Digital Economy. Frost & Sullivan Reports.

[26] Garcia, R. (2020). The Role of Leadership in Developing a Risk-Aware Culture in the Philippine ICT Industry. *Asian Journal of Information Technology, 13*(2), 112-130.

[27] Genovesi, S. (2025). Introducing an AI Governance Framework in Financial Organizations. Best Practices in Implementing the EU AI Act (Practitioner Track). In Symposium on Scaling AI Assessments (SAIA 2024) (pp. 9-1). Schloss Dagstuhl–Leibniz-Zentrum für Informatik. https://doi.org/10.4230/OASIcs.SAIA.2024.9

[28] GlobalData. (2021). Challenges in Data Center Sustainability in Southeast Asia. GlobalData Reports.

[29] Globe Telecom. (2022). Data Center Investments and Growth in the Philippines. Globe Corporate Reports.

[30] Gong, M. Z., & Subramaniam, N. (2020). Principal leadership style and school performance: mediating roles of risk management culture and management control systems use in Australian schools. *Accounting & Finance, 60*(3), 2427-2466. https://doi.org/10.1111/acfi.12416

[31] Grebe, G. P. M., & Marx, J. (2023). The Perceived Relationship between Risk Culture and Operational Risk Management Practices of Ghanaian Banks. *Journal of Risk and Financial Management, 16*(9), 407. https://doi.org/10.3390/jrfm16090407

[32] Hao, Y., Guo, Y., & Wu, H. (2022). The role of information and communication technology on green total factor energy efficiency: does environmental regulation work?. *Business Strategy and the Environment, 31*(1), 403-424. https://doi.org/10.1002/bse.2901

[33] Heo, P. S., & Lee, D. H. (2019). Evolution of the linkage structure of ICT industry and its role in the economic system: The case of Korea. *Information technology for development, 25*(3), 424-454. https://doi.org/10.1080/02681102.2018.1470486

[34] Hernandez, A. A. (2020). Exploring the factors to green IT adoption of SMEs in the Philippines. In Start-Ups and SMEs: Concepts, Methodologies, Tools, and Applications (pp. 907-926). IGI Global.

[35] Hernandez, A. A., & Ona, S. E. (2019). Green IT adoption: lessons from the Philippines business process outsourcing industry. In Green

Business: Concepts, Methodologies, Tools, and Applications (pp. 88-124). IGI Global.

[36] Hoefer, E. R. I. C. H., Cooke, M. A. R. K., & Curry, T. H. O. M. A. S. (2020, August). Three lines of defense—Failed promises and what comes next. In Reuters. Financial Regulatory Forum, September (Vol. 8).

[37] Hu, B., & Denizkurdu, A. (2020). Risk governance framework and the three lines of defence construct: A challenged self-assessment process through an activity-based approach. *Journal of Risk Management in Financial Institutions, 13*(3), 212-223.

[38] Huang, L., Ma, M., & Wang, X. (2022). Clan culture and risk-taking of Chinese enterprises. China Economic Review, 72, 101763. https://doi.org/10.1016/j.chieco.2022.101763

[39] Illahi, A. A. C., Culaba, A., & Dadios, E. P. (2019, November). Internet of Things in the Philippines: a review. In 2019 IEEE 11th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM) (pp. 1-6). IEEE. doi: 10.1109/HNICEM48295.2019.9072882.

[40] Institute of Internal Auditors (IIA). (2013). The Three Lines of Defense in Effective Risk Management and Control.

[41] Institute of Internal Auditors (IIA). (2020). The Three Lines Model: An Update of the Three Lines of Defense. IIA.

[42] Institute of Internal Auditors. (2013). The Three Lines of Defense in Effective Risk Management and Control. Retrieved from https://www.iia.org.uk/media/1698458/three-lines-of-defense.pdf

[43] Institute of Risk Management (IRM). (2018). Risk Culture: Resources for Practitioners.

[44] Institute of Risk Management (IRM). (2020). Leadership and Risk Culture: Building a Resilient Organization. IRM Risk Reports.

[45] International Association of Privacy Professionals (IAPP). (2022). Transparency in Data Privacy Practices: ICT Industry Implications. IAPP Global Privacy Briefing.

[46] International Finance Corporation (IFC). (2021). "Investing in Data Centers for Emerging Markets: The Case of the Philippines. IFC Reports.

[47] International Organization for Standardization (ISO). (2018). ISO 31000: Risk Management Guidelines.

[48] Isabelle, D., Horak, K., McKinnon, S., & Palumbo, C. (2020). Is Porter's Five Forces Framework Still Relevant? A study of the capital/labour intensity continuum via mining and IT industries. *Technology Innovation Management Review, 10*(6).

[49] Jauhiainen, T., & Lehner, O. M. (2022). Good governance of AI and big data processes in accounting and auditing. In Artificial ntelligence in Accounting (pp. 119-181). Routledge.

[50] Kabigting, P. (2023). Training for Data Privacy Compliance in Philippine SMEs. *Journal of Business and Information Technology.*

[51] Kahler, T. (2020, October). Internal Audit, DPO and the adjustment of Three-Lines-of-Defense-Modell. In Turning Point in Data Protection Law (pp. 163-166). Nomos Verlagsgesellschaft mbH & Co. KG.

[52] Kheswa, V. (2023). Risk reporting compliance in the South African banking sector (Doctoral dissertation, North-West University (South Africa)). https://orcid.org/0000-0001-7727-3646

[53] Kim, J., Torneo, A. R., & Yang, S. B. (2019). Philippine readiness for the 4th industrial revolution: A case study. Asia-Pacific Social Science Review, 19(1), 10. DOI: https://doi.org/10.59588/2350-8329.1206

[54] Kucharska, W. (2021). Do mistakes acceptance foster innovation? Polish and US cross-country study of tacit knowledge sharing in IT. *Journal of Knowledge Management, 25*(11), 105-128. https://doi.org/10.1108/JKM-12-2020-0922

[55] Kumar, S., & Anbanandam, R. (2020). Impact of risk management culture on supply chain resilience: An empirical study from Indian manufacturing industry. Proceedings of the Institution of Mechanical Engineers, Part O: *Journal of Risk and Reliability, 234*(2), 246-259. https://doi.org/10.1177/1748006X1988671

[56] Kumari, R., & Singh, S. K. (2024). Impact of ICT infrastructure, financial development, and trade openness on economic growth: New evidence from low-and high-income countries. *Journal of the Knowledge Economy, 15*(2), 7069-7098. https://doi.org/10.1007/s13132-023-01332-

[57] Kurniawati, M. A. (2020). The role of ICT infrastructure, innovation and globalization on economic growth in OECD countries, 1996-2017. *Journal of Science and Technology Policy Management, 11*(2), 193-215. https://doi.org/10.1108/JSTPM-06-2019-0065

[58] Migliorelli, M., & Marini, V. (2020). Sustainability-related risks, risk management frameworks and non-financial disclosure. Sustainability and financial risks: The impact of climate change, environmental degradation and social inequality on financial markets, 93-118. https://doi.org/10.1007/978-3-030-54530-7_4

[59] Mihardjo, L., Sasmoko, S., Alamsjah, F., & Elidjen, E. (2019). Digital leadership role in developing business model innovation and customer experience orientation in industry 4.0. *Management Science Letters, 9*(11), 1749-1762. DOI: 10.5267/j.msl.2019.6.015

[60] Milić, M., Borocki, J., & Vekić, A. (2024, May). The Power of ICT Infrastructure in Fostering Innovation Development. In 2024 47th MIPRO ICT and Electronics Convention (MIPRO) (pp. 1905-1910). IEEE. doi: 10.1109/MIPRO60963.2024.10569834.

[61] Minter, R. (2019). The Influence of Leadership on Regulatory Compliance and Risk Culture. *Risk and Compliance Journal, 14*(1), 37-52.

[62] Molelekoa, T. I. (2022). Evaluation of enterprise risk management culture at lesotho highlands development authority. http://hdl.handle.net/11660/12216

[63] National Institute of Standards and Technology (NIST). (2018). NIST Cybersecurity Framework.

[64] National Privacy Commission (NPC). (2021). Data Privacy and SMEs: Bridging the Compliance Gap." NPC Bulletin.

[65] National Privacy Commission. (2023). NPC Data Privacy Guidelines for ICT Firms. Retrieved from https://www.privacy.gov.ph

[66] Niyafard, S., Jalalian, S. S., Damirchi, F., Jazayerifar, S., & Heidari, S. (2024). Exploring the impact of information technology on the relationship between management skills, risk management, and project success in construction industries. *International Journal of Business Continuity and Risk Management, 14*(2), 97-118. https://doi.org/10.1504/IJBCRM.2024.139032

[67] Novaes Neto, N., Madnick, S., de Paula, M. G., & Malara Borges, N. (2020). A case study of the capital one data breach. Stuart E. and Moraes G. de Paula, Anchises and Malara Borges, Natasha, A Case Study of the Capital One Data Breach (January 1, 2020). http://dx.doi.org/10.2139/ssrn.3542567

[68] Olaniyi, O. O., & Omubo, D. S. (2023). The importance of COSO framework compliance in information technology auditing and enterprise resource management. *International Journal of Innovative Research & Development, 12*(4). https://ssrn.com/abstract=4546206

[69] Organisation for Economic Co-operation and Development (OECD). (2020). "ICT and Innovation Ecosystems in the Asia-Pacific." OECD

Studies.

[70] Pantos, S. Supervisory Approaches to AI Regulation in Insurance: The Case of the UK Prudential Framework. In Organizations and Technology for Sustainability (pp. 80-112). CRC Press.

[71] Park, H., & Choi, S. O. (2019). Digital innovation adoption and its economic impact focused on path analysis at national level. *Journal of open innovation: Technology, market, and complexity, 5*(3), 56. https://doi.org/10.3390/joitmc5030056

[72] Park, Y. J. (2019). Risk Culture and Risk Management in the Australian Public Sector (Doctoral dissertation, The Australian National University (Australia)).

[73] Patipan, S. L. (2024). Modeling Enterprise Risk Management Ecosystems Using Text Analytics. *Foundations of Management, 16*(1), 391-406. DOI:10.2478/fman-2024-0024

[74] Pecina, E., Miloš Sprčić, D., & Dvorski Lacković, I. (2022). Qualitative analysis of enterprise risk management systems in the largest European electric power companies. *Energies, 15*(15), 5328. https://doi.org/10.3390/en15155328

[75] Peraković, D., Periša, M., & Zorić, P. (2019). Challenges and Issues of ICT in Industry 4.0. Design, simulation, manufacturing: The innovation exchange, 259-269. https://doi.org/10.1007/978-3-030-22365-6_26

[76] PwC. (2021). Cybersecurity and the Three Lines of Defense: Navigating regulatory compliance in the digital era. PwC Global Risk Report.

[77] PwC. (2021). Risk Governance in the Digital Age: Managing ICT Industry Compliance.

[78] PwC. (2021). The Three Lines of Defense: Enhancing Risk Management and Control Through Technology.

[79] Ratnasari, S. L., Prasetiyo, E. J., & Hakim, L. (2020). The effect of organizational commitment, organizational culture, work environment, and leadership style on job satisfaction. Enrichment: Journal of Management, 11(1, Novembe), 57-62. https://doi.org/10.35335/enrichment.v11i1,%20Novembe.27

[80] Reyes, J. (2022). "SME Compliance with the Data Privacy Act: Challenges and Solutions." *Philippine Journal of Data Privacy.*

[81] Saeidi, P., Saeidi, S. P., Sofian, S., Saeidi, S. P., Nilashi, M., & Mardani, A. (2019). The impact of enterprise risk management on competitive advantage by moderating role of information technology. *Computer standards & interfaces, 63*, 67-82. https://doi.org/10.1016/j.csi.2018.11.009

[82] Sarangi, A. K., & Pradhan, R. P. (2020). ICT infrastructure and economic growth: A critical assessment and some policy implications. *Decision, 47*(4), 363-383. https://doi.org/10.1007/s40622-020-00263-5

[83] Seidenfuss, K. U., Young, A., & Datwani, M. (2023). Integrating governance, risk and compliance? A multi-method analysis of the new Three Lines Model. SN Business & Economics, 3(10), 184. https://doi.org/10.1007/s43546-023-00561-x

[84] Solid Waste Management Commission (SWMC). (2019). "Recycling Programs and E-Waste Regulations in ICT." SWMC Bulletin.

[85] Song, M., Wang, S., & Zhang, H. (2020). Could environmental regulation and R&D tax incentives affect green product innovation?. *Journal of Cleaner Production, 258*, 120849. https://doi.org/10.1016/j.jclepro.2020.120849

[86] Sun, H., & Kim, G. (2021). The composite impact of ICT industry on lowering carbon intensity: from the perspective of regional heterogeneity. Technology in Society, 66, 101661. https://doi.org/10.1016/j.techsoc.2021.101661

[87] Tambouris, E., Zeginis, D., Matziaras, G., Stefanidis, N., Promikyridis, R., Tarabanis, K., ... & Bodino, M. C. (2024). Using the EU Big Data Test Infrastructure to Publish MITOS Public Service Descriptions as Linked Open Data.

[88] Tammenga, A. (2020). The application of Artificial Intelligence in banks in the context of the three lines of defence model. Maandblad Voor Accountancy en Bedrijfseconomie, 94(5/6), 219-230. https://doi.org/10.5117/mab.94.47158

[89] Tone, B. (2018). Leadership and Risk Culture: How Management Affects Risk Behavior. *Journal of Risk and Governance, 12*(3), 155-178.

[90] Turk, Ž., Sonkor, M. S., & Klinc, R. (2022). Cybersecurity assessment of BIM/CDE design environment using cyber assessment framework. *Journal of Civil Engineering and Management, 28*(5), 349-364. https://doi.org/10.3846/jcem.2022.16682

[91] Turner, D. (2022). Three lines of defence—is it the right model?. *Journal of Financial Compliance, 5*(3), 237-247.

[92] United Nations Conference on Trade and Development (UNCTAD). (2020). Digital Economy Report 2020: Cross-border Data Flows and Development.

[93] United Nations Conference on Trade and Development (UNCTAD). (2022). Cybersecurity and Data Privacy in Southeast Asia: Policy Trends and Challenges. UNCTAD.

[94] United Nations Conference on Trade and Development (UNCTAD). (2021). Digital Economy Report 2021: Data and Digitalization for Development.

[95] Uy-Tioco, C. S. (2019). 'Good enough'access: digital inclusion, social stratification, and the reinforcement of class in the Philippines. *Communication Research and Practice, 5*(2), 156-171. https://doi.org/10.1080/22041451.2019.1601492

[96] Vaughan, C. (2022). Financial crime compliance in professional services: Moving beyond the three lines of defence. *Journal of Financial Compliance, 5*(3), 267-274.

[97] Verma, P., & Kumar, V. (2022). Developing leadership styles and green entrepreneurial orientation to measure organization growth: a study on Indian green organizations. Journal of Entrepreneurship in Emerging Economies, 14(6), 1299-1324. https://doi.org/10.1108/JEEE-01-2021-0035

[98] Wall, A. M. (2021). Guidelines for artificial intelligence-driven enterprise compliance management systems (Doctoral dissertation). https://doi.org/10.17869/enu.2022.2850798

[99] Walter, S., & Narring, F. (2020). How can supervisors and banks promote a culture of strong governance and ethical behaviour?. Journal of Risk Management in Financial Institutions, 13(2), 145-154.

[100]Zeier Röschmann, A., Barth, S., Wipf, D., & Meienberger, F. (2019). Insights into challenges and trends relating to the'three lines of defence'model at Swiss insurance companies. https://digitalcollection.zhaw.ch/handle/11475/20171