Online at www.e-iph.co.uk
Indexed in Clarivate Analytics WoS, and ScienceOPEN

E-B Environment - Behaviour Proceedings Journal

KICSS2024

Kedah International Conference on Social Sciences

https://kicss2024.wixsite.com/kicss2024

e-IPH e-International Publishing House Ltd., United Kingdom

InforMaTIC2024: Information Management and Technology International Conference
Virtual Conference, UiTM Kedah, Malaysia

Organised by: Universiti Teknologi MARA, Kedah, Malaysia

Exploring Critical Success Factors in Compliance-Driven Cyber Insurance within Malaysian Organizations: A COBIT 5 Enabler approach

Nor Hasnul Azirah Abdul Hamid[1]*, Mazita Mokhtar[2], Wan Khairul Anuar Wan Abd Manan[2], Husna Hashim[2]
**Corresponding Author*

[1] Faculty of Computer and Mathematical Sciences, UiTM Cawangan Terengganu Kampus Kuala Terengganu, Malaysia,
[2] Faculty of Industrial Management, Universiti Malaysia Pahang Al-Sultan Abdullah, Malaysia.

hasnulazirah@uitm.edu.my, mazita@umpsa.edu.my, anuar@umpsa.edu.my, husnahashim@umpsa.edu.my
Tel: +6019 3972298

Abstract
In today's cybersecurity landscape, cyber insurance is only effective when aligned with established frameworks and regulatory compliance. Hence, this study explores the critical success factors (CSFs) for implementing compliance-driven cyber insurance in Malaysian organizations using the COBIT 5 enabler framework. Based on semi-structured interviews with eight industry experts, the thematic analysis identified ten key themes and seventeen sub-themes mapped to the seven COBIT 5 enablers. The findings propose a structured framework that aligns cybersecurity compliance strategies with COBIT 5 to facilitate effective cyber insurance adoption. These insights offer theoretical and practical contributions to cyber risk governance and compliance-oriented cybersecurity planning.

Keywords: cyber insurance; compliance-driven; critical success factors; COBIT 5 enablers.

DOI: https://doi.org/10.21834/e-bpj.v10iSI31.6936

1.0 Introduction

Organizations face rising cyber threats alongside growing regulatory pressure, making cyber insurance a key cybersecurity strategy. In Malaysia, regulators such as Bank Negara Malaysia (BNM), CyberSecurity Malaysia, and the Department of Personal Data Protection (JPDP) are reinforcing mandates for cyber insurance, particularly in finance, healthcare, and critical infrastructure sectors (Abdul Hamid et al., 2022). The global cyber insurance market is projected to grow from USD 13.13 billion in 2024 to USD 68.35 billion by 2030 (Rangu et al., 2024). However, policy coverage alone is insufficient; its effectiveness depends on compliance with standards and frameworks (Cremer et al., 2024; Mott et al., 2023).

This has led to the emergence of compliance-driven cyber insurance, where policies are developed and assessed in line with legal, regulatory, and industry-specific frameworks. Frameworks such as COBIT 5, ISO/IEC 27001, and the NIST Cybersecurity Framework embed cyber insurance within IT governance and risk management. Despite its importance, there is limited research on how compliance enables cyber insurance implementation in Malaysia.

Previous studies (Yeoh et al., 2022; Diesch et al., 2020; Wrede et al., 2020) have explored cyber insurance challenges but rarely treat compliance as a central enabler. To address this gap, this study investigates the critical success factors (CSFs) influencing

eISSN: 2398-4287 © 2025. The Authors. Published for AMER by e-International Publishing House, Ltd., UK. This is an open access article under the CC BY-NC-ND license (http://c5eativecommons.org/licenses/by-nc-nd/4.0/). Peer–review under responsibility of AMER (Association of Malaysian Environment-Behaviour Researchers
DOI: https://doi.org/10.21834/e-bpj.v10iSI31.6936

compliance-driven cyber insurance, using COBIT 5 as a guiding framework. The study aims to: (1) identify the key CSFs that enable effective implementation of compliance-driven cyber insurance; (2) align the identified CSFs with the seven enablers of the COBIT 5 framework; and (3) develop a theoretical framework that maps these CSFs to COBIT 5 to support structured, compliance-aligned cyber insurance implementation in Malaysian organizations.

2.0 Literature Review

2.1 Cyber Insurance

Cyber insurance is now a key element of organizational risk management, providing financial protection against cyber threats like ransomware, data breaches, and business disruptions (Abdul Hamid et al., 2022; Mott et al., 2023). While global research explores adoption drivers, concerns persist over exclusions, high premiums, and delayed claims (Cremer et al., 2024; Dambra et al., 2020). In Malaysia, adoption remains low, particularly among SMEs, due to limited awareness, regulatory complexity, and resource constraints (Abdul Hamid et al., 2022; Abd Rahman et al., 2022). Although previous studies examine these challenges, they often do so in isolation. The integration of CSFs with compliance-oriented governance frameworks like COBIT 5 remains underexplored, particularly in Malaysia's regulatory environment.

2.2 COBIT 5 (Control Objectives for Information and Related Technologies) Enablers

COBIT 5, developed by ISACA (2012), is a globally recognized governance framework that includes seven enablers supporting the alignment of IT, risk, and compliance. These enablers can guide the integration of cyber insurance into broader compliance strategies. A compliance-driven approach treats cyber insurance not as a standalone product but as part of a holistic risk governance model (Wallace et al., 2020), enhancing organizational preparedness. Table 1 summarizes the COBIT 5 enablers.

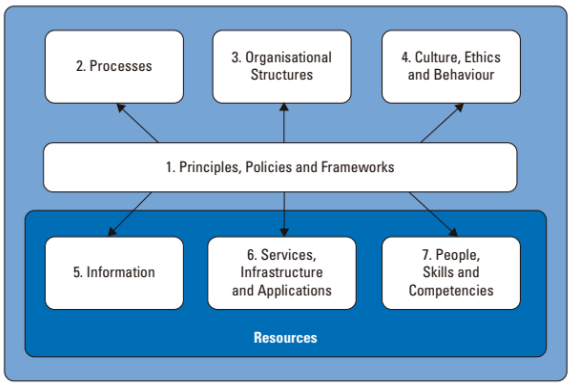

Fig. 1: COBIT 5 Enterprise Enablers in COBIT 5 Framework.
(Source: ISACA, 2012)

Table 1. Explanation of the Seven COBIT 5 Enablers

Enablers	Explanation
Process	Structured, repeatable IT tasks to meet goals.
Organizational Structures	Clear roles and responsibilities for governance.
Culture, Ethics, and Behaviour	Promotes ethical, governance-aligned behavior.
Principles, Policies, and Frameworks	Foundations guiding IT decisions and alignment.
Information	Secure, efficient data management as a key asset.
Services, Infrastructure, and Applications	Ensures necessary IT systems and tools are in place.
People, Skills, and Competencies	Skilled personnel for effective IT governance.

(Source: ISACA, 2012)

2.3 Critical Success Factors (CSFs) in Compliance-Driven Cyber Insurance

CSFs are key elements that ensure the successful adoption of compliance-driven cyber insurance. Seventeen CSFs (see Table 2) have been identified as crucial to this process, with academic references supporting each factor.

Table 2. Supporting Academic References for Critical Success Factors in Compliance-Driven Cyber Insurance Adoption

Critical Success Factors (CSFs) in Cyber Insurance Adoption	Supporting Academic References
Understanding Regulatory Requirements	Cremer et al. (2024); Abd Rahman et al. (2022); Abdul Hamid et al. (2022); Schlackl et al. (2022); Hasan et al. (2021); Markopoulou, (2021); Lemnitzer (2021); Aziz et al. (2020); Kshetri (2020); Zeller and Scherer (2020)
Aligning Cyber Insurance Policies with Regulations	Cremer et al. (2024); Markopoulou (2021); Wrede et al. (2020)
Tailored Coverage Options	Schütz et al. (2023); Abdul Hamid et al. (2022); Zeller and Scherer (2020)

Exclusions and Limitations	Cremer et al. (2024); Mott et al., 2023; Schütz et al. (2023); Abd Rahman et al. (2022); Abdul Hamid et al. (2022); Markopoulou, (2021); Aziz et al. (2020); Kshetri (2020); Wrede et al. (2020); Zeller and Scherer (2020)
Risk Assessment and Identification	Cremer et al. (2024); Rangu et al. (2024); Mott et al., 2023; Schütz et al. (2023); Abd Rahman et al. (2022); Schlackl (2022); Hasan et al. (2021); Markopoulou, (2021); Aziz et al. (2020); Kshetri (2020); Wrede et al. (2020); Zeller and Scherer (2020)
Quantification of Cyber Risks	Rangu et al. (2024); Schlackl (2022); Kshetri (2020); Zeller and Scherer (2020)
Budget Allocation	Hasani et al. (2023); Markopoulou (2021); Aziz et al. (2020)
Cost-Benefit Analysis	Mott et al., 2023; Markopoulou (2021); Aziz et al. (2020); Dambra et al. (2020); Zeller and Scherer (2020)
Executive Leadership and Governance	Mott et al., 2023; Abdul Hamid et al. (2022); Hasan et al. (2021)
Cross-Departmental Collaboration	Hasan et al. (2021); Wallace et al. (2020)
Compliance with Legal Obligations	Cremer et al. (2024); Mott et al., 2023; Schütz et al. (2023); Abd Rahman et al. (2022); Abdul Hamid et al. (2022); Schlackl (2022); Hasan et al. (2021); Markopoulou, (2021); Aziz et al. (2020); Kshetri (2020); Zeller and Scherer (2020)
Transparency with Regulators and Insurers	Cremer et al. (2024); Zeller and Scherer (2020)
Continuous Monitoring and Improvement	Cremer et al. (2024); Schütz et al. (2023); Abd Rahman et al. (2022); Markopoulou, (2021); Kshetri (2020);
Managing data in compliance with cybersecurity and regulatory requirements.	Rangu et al. (2024); Cremer et al. (2024); Mott et al., 2023; Abdul Hamid et al. (2022);
Data Integrity and Availability	Schlackl (2022); Hasan et al. (2021); Markopoulou, (2021);
Integration with IT Systems	Cremer et al. (2024); Mott et al., 2023; Abd Rahman et al. (2022); Abdul Hamid et al. (2022); Hasan et al. (2021); Aziz et al. (2020); Kshetri (2020); Wrede et al. (2020); Zeller and Scherer (2020)
Employee Training on Compliance of Cyber Insurance	Abdul Hamid et al. (2022); Zeller and Scherer (2020)

Understanding regulatory requirements is foundational for aligning cyber insurance policies with national and international standards (Cremer et al., 2024; Abdul Rahman et al., 2022), though this is often complex for multinational organizations managing diverse regulatory environments (Wrede et al., 2020). Effective risk assessment and quantification models enable tailored coverage (Schütz et al., 2023; Kshetri, 2020), while clear understanding of policy exclusions helps avoid disputes and build trust with insurers (Mott et al., 2023; Aziz et al., 2020). Executive leadership and governance are crucial for integrating cyber insurance into broader risk strategies (Mott et al., 2023; Abdul Hamid et al., 2022), supported by cross-departmental collaboration and ongoing policy reviews that enhance organizational adaptability to evolving threats (Hasan et al., 2021; Cremer et al., 2024).

Although these CSFs are acknowledged, they are often considered to be isolated and lack integration within a structured governance model. Notably, limited research explores how these factors align with compliance frameworks such as COBIT 5. This study addresses that gap by mapping CSFs onto COBIT 5 enablers, offering a governance-based framework tailored to Malaysia's regulatory context.

3.0 Methodology

The methodology outlined in this study is designed to explore the CSFs in compliance-driven cyber insurance within Malaysian organizations, using the COBIT 5 Enabler approach as the guiding framework (refer to Fig. 2).

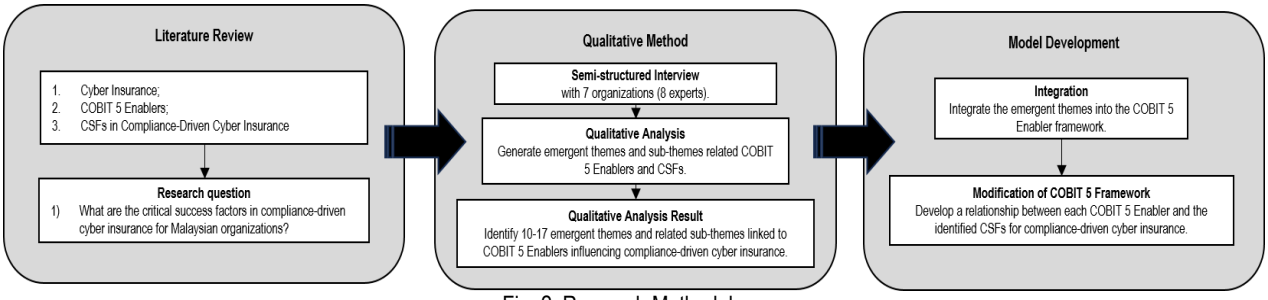

Fig. 2: Research Methodology

This study employed a three-phase qualitative methodology: literature review, expert interviews, and model development. The literature review focused on cyber insurance, COBIT 5 enablers, and CSFs in compliance-driven adoption. In the empirical phase, eight experts from seven Malaysian organizations were purposively selected based on roles in cybersecurity, risk, and insurance. Sampling was guided by the "information power" principle (Malterud et al., 2016), suitable for focused, expertise-driven studies. Thematic saturation was achieved after six interviews, with two additional interviews confirming data consistency. Semi-structured interviews examined three areas: (1) understanding of cyber insurance, (2) COBIT 5 enablers' role, and (3) organizational challenges and CSFs. Ethical approval was obtained, and informed consent was secured. Data were analyzed using Braun and Clarke's (2006) six-phase approach: (1) familiarization, (2) initial coding, (3) theme generation, (4) theme review, (5) theme definition, and (6) reporting. Gioia et al.'s (2013) method structured findings into first-order concepts, second-order themes, and aggregate dimensions. In the final phase, the identified CSFs were mapped onto COBIT 5 enablers to develop a governance-aligned model. Potential bias from qualitative interpretation was mitigated through dual coding and peer debriefing, ensuring analytical rigor.

4.0 Findings

4.1 Emergent Themes related to Critical Success Factors (CSFs) in Compliance-Driven Cyber Insurance

Based on qualitative data analysis, ten themes emerged (see Fig. 3) related to the CSFs in compliance-driven cyber insurance.

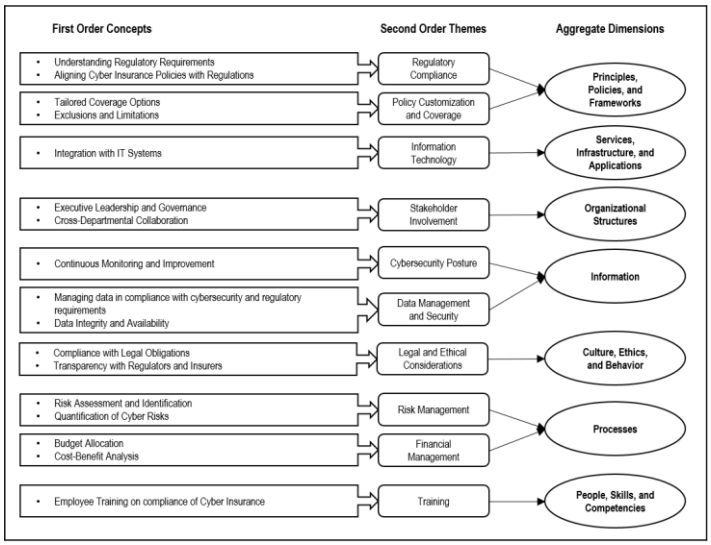

Fig. 3: Emergent Themes Related to CSFs in Compliance-Driven Cyber Insurance

4.1.1 Principles, Policies, and Frameworks

This study underscores the importance of regulatory compliance in cyber insurance adoption, particularly aligning with Malaysian laws like the Personal Data Protection Act (PDPA). Seven of the eight respondents (R1, R2, R3, R4, R6, R7, R8) emphasized understanding cybersecurity regulations, with R4 noting that compliance teams enhance preparedness. Four respondents (R3, R4, R7, R8) highlighted that regulatory alignment strengthens cyber resilience. Policy customization was also key, with three (R4, R5, R6) stressing that generic policies fail to meet industry-specific needs. One (R6) from banking emphasized tailored coverage. Three respondents noted exclusions require negotiation. Overall, 87.5% emphasized compliance, and 62.5% emphasized customization as a critical adoption factor.

Table 3. Principles, Policies, And Frameworks: Critical Success Factors (CSFs) And Corresponding Codes

Critical Success Factors (CSFs) (Themes)	No. of Codes for each Respondent	Total Respondents (Max. 8 Respondents)
Regulatory Compliance		
Understanding Regulatory Requirements	R1**, R2**, R3*, R4*, R6***, R7*, R8**	7
Aligning Cyber Insurance Policies with Regulations	R3**, R4****, R7***, R8**	4
Cumulative	*R1, R2, R3, R4, R6, R7, R8*	*7/8 (87.5%)*
Policy Customization and Coverage		
Tailored Coverage Options	R4**, R5***, R6**	
Exclusions and Limitations	R2*, R3*, R4***	
Cumulative	*R2, R3, R4, R5, R6*	*5/8 (62.5%)*
*Notes: R1 – R8 = respondents; * = no. of references on transcript text*		

4.1.2 Services, Infrastructure, and Applications

Integrating cyber insurance with existing IT systems is vital for effective implementation and monitoring. Six of eight respondents (R2, R3, R4, R5, R7, R8) emphasized that aligning insurance with IT infrastructure improves compliance and operational efficiency. Embedding insurance into tools like security information and event management (SIEM) and asset management systems enables real-time monitoring, quicker threat response, and regulatory adherence. This positions cyber insurance as a proactive IT strategy component. Overall, 75% of respondents viewed this integration as critical for adoption success.

Table 4. Services, Infrastructure, and Applications: Critical Success Factors (CSFs) and Corresponding Codes

Critical Success Factors (CSFs) (Themes)	No. of Codes for each Respondent	Total Respondents (Max. 8 Respondents)
Information Technology		
Integration with IT Systems	R2*, R3***, R4*, R5***, R7*, R8**	6
Cumulative	R2, R3, R4, R5, R7, R8	6/8 (75%)
*Notes: R1 – R8 = respondents; * = no. of references on transcript text*		

4.1.3 Organizational Structures

Executive leadership and governance are crucial for compliance-driven cyber insurance, emphasized by 7 of 8 respondents (R1, R2, R4, R5, R6, R7, R8). Strong leadership drives cybersecurity efforts and embeds compliance into governance. Cross-departmental collaboration, noted by four respondents (R2, R5, R7, R8), involving IT, legal, compliance, and finance, supports effective policy execution. One respondent (R3) cited the collaboration between BNM and CyberSecurity Malaysia as a national model. In total, 87.5% of participants viewed leadership and collaboration as critical for successful implementation.

Table 5. Organizational Structures: Critical Success Factors (CSFs) and Corresponding Codes

Critical Success Factors (CSFs) (Themes)	No. of Codes for each Respondent	Total Respondents (Max. 8 Respondents)
Stakeholder Involvement		
Executive Leadership and Governance	R1*, R2**, R4*, R5***, R6**	7
Cross-Departmental Collaboration	R2*, R5**, R7*, R8*	4
Cumulative	*R1, R2, R4, R5, R6, R7, R8*	*7/8 (87.5%)*
*Notes: R1 – R8 = respondents; * = no. of references on transcript text*		

4.1.4 Information

Analysis of the "Information" dimension reveals two key themes: Cybersecurity Posture and Data Management. Half of the respondents (R5, R6, R7, R8) stressed that continuous monitoring, including vulnerability assessments and real-time threat detection, is vital for compliance-driven cyber insurance. Equally important is adherence to data regulations, five of eight respondents (62.5%) emphasized compliance with standards like the PDPA. Three participants (R2, R4, R5) highlighted the need to maintain data integrity and availability. These information-focused practices significantly enhance readiness, compliance, and resilience, making them critical to effective cyber insurance adoption.

Table 6. Information: Critical Success Factors (CSFs) and Corresponding Codes

Critical Success Factors (CSFs) (Themes)	No. of Codes for each Respondent	Total Respondents (Max. 8 Respondents)
Cybersecurity Posture		
Continuous Monitoring and Improvement	R5*, R6**, R7**, R8*	4
Cumulative	*R5, R6, R7, R8*	*4/8 (50%)*
Data Management and Security		
Managing data in compliance with cybersecurity and regulatory requirements	R1**, R4*, R5*	
Data Integrity and Availability	R2**, R4**, R5**, R6*	
Cumulative	*R1, R2, R4, R5, R6*	*5/8 (62.5%)*
*Notes: R1 – R8 = respondents; * = no. of references on transcript text*		

4.1.5 Culture, Ethics, and Behavior

Culture, ethics, and behavior are vital for compliance-driven cyber insurance, particularly in addressing legal and ethical responsibilities. Three respondents (R3, R7, R8) emphasized legal compliance, supported by legal teams and internal audits to align with evolving cybersecurity regulations. This approach builds trust and strengthens risk management. Transparency was also key, three respondents (R1, R6, R7) noted that open communication with regulators and insurers enhances compliance readiness and improves policy terms. Together, these factors reinforce stakeholder confidence and resilience. Overall, 5 of 8 respondents (62.5%) highlighted legal and ethical considerations as essential for successful adoption.

Table 7. Culture, Ethics, and Behavior: Critical Success Factors (CSFs) and Corresponding Codes

Critical Success Factors (CSFs) (Themes)	No. of Codes for each Respondent	Total Respondents (Max. 8 Respondents)
Legal and Ethical Considerations		
Compliance with Legal Obligations	R3***, R7*, R8**	
Transparency with Regulators and Insurers	R1**, R6*, R7****	
Cumulative	*R1, R3, R6, R7, R8*	*5/8 (62.5%)*
*Notes: R1 – R8 = respondents; * = no. of references on transcript text*		

4.1.6 Processes

Risk assessment and identification are fundamental to compliance-driven cyber insurance, with seven of eight respondents (R1–R7) stressing the need to evaluate threats by impact and likelihood. Frameworks like ISO/IEC 27001 (cited by R2, R5, R6) support structured risk management. Four respondents (R1, R5, R6, R8) highlighted quantifying risks to justify insurance investments. All respondents (100%) agreed risk management is critical. Financial management also emerged as key, with 87.5% noting challenges in budget allocation (R3, R4, R6, R8) and the importance of cost-benefit analysis (R1, R5, R7) guided by frameworks like BNM's Risk Management in Technology (RMiT).

Table 8. Processes: Critical Success Factors (CSFs) and Corresponding Codes

Critical Success Factors (CSFs) (Themes)	No. of Codes for each Respondent	Total Respondents (Max. 8 Respondents)
Risk Management		
Risk Assessment and Identification	R1*, R2***, R3**, R4*, R5*, R6***, R7*, R8**	7
Quantification of Cyber Risks	R1**, R5***, R6**, R8**	4
Cumulative	*R1, R2, R3, R4, R5, R6, R7, R8*	*8/8 (100%)*
Financial Management		
Budget Allocation	R3*, R4**, R6**, R8*	
Cost-Benefit Analysis	R1*, R5*, R7*	
Cumulative	*R1, R3, R4, R5, R6, R7, R8*	*7/8 (87.5%)*
*Notes: R1 – R8 = respondents; * = no. of references on transcript text*		

4.1.7 People, Skills, and Competencies

Employee training is a critical component of cyber insurance strategies, with 7 out of 8 respondents (87.5%) emphasizing its importance. Training ensures staff understand both insurance policies and regulatory obligations. One respondent (R2) noted that it enhances compliance awareness. Organizations are increasingly adopting customized, department-specific training to address varying roles and responsibilities. This targeted approach ensures that all employees are equipped with the relevant knowledge needed for the effective implementation of compliance-driven cyber insurance.

Table 9. People, Skills, and Competencies: Critical Success Factors (CSFs) and Corresponding Codes

Critical Success Factors (CSFs) (Themes)	No. of Codes for each Respondent	Total Respondents (Max. 8 Respondents)
Training		
Employee Training on Compliance of Cyber Insurance	R1*, R2*, R3**, R4*, R5***, R7*, R8**	7
Cumulative	R1, R2, R3, R4, R5, R7, R8	7/8 (87.5%)
*Notes: R1 – R8 = respondents; * = no. of references on transcript text*		

4.2 Adapting the COBIT 5 Enabler for Critical Success Factors (CSFs) in Compliance-Driven Cyber Insurance

Based on the COBIT 5 enablers from ISACA (2012), this theoretical framework (refer to Fig.4) maps CSFs across seven enablers, each representing essential organizational elements required for effective implementation and regulatory compliance in Malaysian compliance-driven cyber insurance.

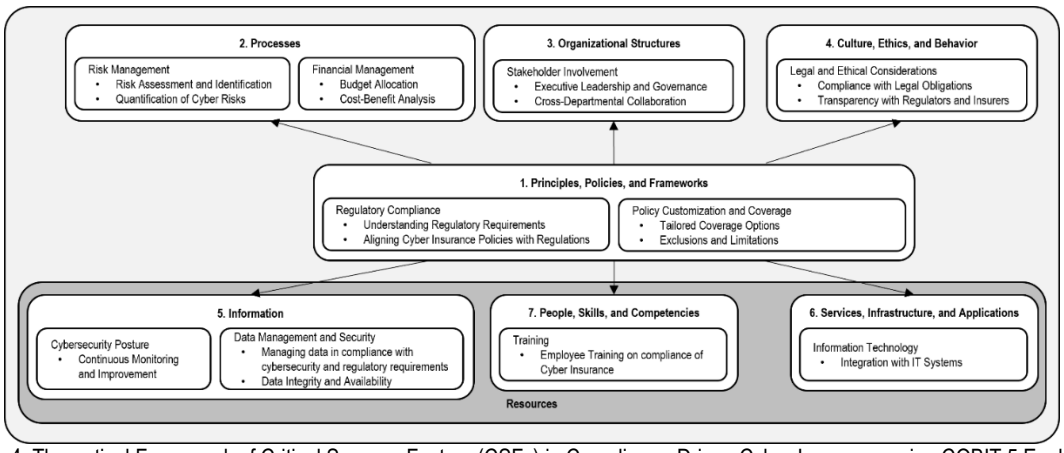

Fig. 4: Theoretical Framework of Critical Success Factors (CSFs) in Compliance-Driven Cyber Insurance using COBIT 5 Enabler

5.0 Discussion

This study offers new insights into operationalizing compliance-driven cyber insurance through the COBIT 5 enabler framework. By mapping seventeen critical success factors (CSFs) to seven governance enablers, the findings emphasize that cyber insurance effectiveness depends not merely on policy acquisition but on embedding it within governance, compliance, and operational systems. Theoretically, the study extends COBIT 5 beyond traditional IT governance to a strategic tool for aligning cyber insurance with compliance and enterprise risk management. It integrates institutional theory, highlighting regulatory mandates like Malaysia's PDPA and BNM's RMiT as coercive forces prompting structured adoption, and socio-technical systems theory, underscoring the need to balance human capabilities with technological infrastructure for effective implementation.

The study also addresses gaps in prior literature, which often isolates cyber insurance barriers, such as cost, exclusions, or awareness. Findings suggest these challenges can be mitigated through structured governance mechanisms. Enablers like executive leadership, policy customization, and real-time monitoring are interdependent and essential for adoption success. Although focused on

Malaysia, the proposed framework is globally relevant. Sectors in the EU, U.S., or ASEAN, particularly finance, healthcare, and energy, can adopt similar strategies. The alignment of Malaysia's PDPA with frameworks like Europe's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA) reinforces the model's cross-border adaptability. Moreover, in developing economies where cyber insurance markets are nascent, this framework provides a structured path toward compliance, risk readiness, and resilience. In summary, the study reframes cyber insurance as an integrated component of organizational governance. The COBIT 5 enabler model presents a scalable approach for aligning insurance with compliance and cybersecurity demands in complex, regulated environments.

6.0 Conclusion& Recommendations

This study identifies CSFs for implementing compliance-driven cyber insurance in Malaysian organizations using the COBIT 5 enabler model. Findings emphasize the need for strategic alignment across governance, regulatory compliance, technology, and human capabilities. Rather than treating cyber insurance as a reactive safeguard, it should be integrated into enterprise-wide compliance and risk frameworks. Organizations are advised to align policies with evolving regulations like PDPA and RMiT, strengthen executive leadership, foster cross-functional collaboration, automate compliance monitoring, conduct regular risk assessments, and deliver targeted employee training to enhance both compliance and resilience.

The qualitative methodology, based on interviews with eight professionals, offers depth but limits generalizability due to sample size and sector focus. Although thematic saturation was achieved, some interpretive bias remains possible despite dual coding and peer debriefing.

Future research should broaden the model's application to SMEs and under-regulated sectors. Cross-jurisdictional comparisons and quantitative methods can validate and prioritize CSFs. Longitudinal studies could track how CSF relevance evolves amid shifting regulatory and cyber threat landscapes.

Acknowledgments

We extend our heartfelt gratitude to the industry experts and regulatory bodies whose insights and guidance were instrumental in shaping this research. We also thank our colleagues and academic mentors for their continuous support and valuable feedback throughout the study.

Paper Contribution to Related Field of Study

This paper contributes to Information System Management by demonstrating how CSFs for successful compliance-driven cyber insurance align with COBIT 5 enablers, thereby strengthening governance and risk management.

References

Abd Rahman, N. H., Raju, R., Ariffin, S., Abdul Hamid, N. H. A., & Ahmad, A. (2022). Adoption of Cyber Insurance in Malaysian Organisations. International Journal of Innovative Computing, 12(2), 45–51. doi: https://doi.org/10.11113/ijic.v12n2.380

Abdul Hamid, N. H. A., Mat Nor, N. I., Hussain, F. M., Raju, R., Naseer, H., & Ahmad, A. (2022). Barriers and Enablers to Adoption of Cyber Insurance in Developing Countries: An Exploratory Study of Malaysian Organizations. Computers & Security, 102893. doi: https://doi.org/10.1016/j.cose.2022.102893

Aziz, B., Suhardi, & Kurnia. (2020). A systematic literature review of cyber insurance challenges. 2020 International Conference on Information Technology Systems and Innovation (ICITSI). doi: https://doi.org/10.1109/icitsi50517.2020.9264966

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. Qualitative Research in Psychology, 3(2), 77–101. doi: https://doi.org/10.1191/1478088706qp063oa

Cremer, F., Sheehan, B., Mullins, M., Fortmann, M., Ryan, B. J., & Materne, S. (2024). On the insurability of cyber warfare: An investigation into the German cyber insurance market. Computers & Security, 142, 103886. doi: https://doi.org/10.1016/j.cose.2024.103886

Dambra, S., Bilge, L., & Balzarotti, D. (2020). SoK: Cyber Insurance – Technical Challenges and a System Security Roadmap. IEEE Xplore. doi: https://doi.org/10.1109/SP40000.2020.00019

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. Computers & Security, 92(1), 101747. doi: https://doi.org/10.1016/j.cose.2020.101747

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research. Organizational Research Methods, 16(1), 15–31.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications, 58(1), 102726. doi: https://doi.org/10.1016/j.jisa.2020.102726

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. SN Business & Economics, 3(5). doi: https://doi.org/10.1007/s43546-023-00477-6

Hwee, L.S., 2009. Cyber Risk Insurance Policy: a Proposed Framework for E-Business in Malaysia. Universiti Teknologi Malaysia [Master dissertation].

Information Systems Audit and Control Association (ISACA) (2012). COBIT 5: enabling processes. ISACA.

Kshetri, N. (2020). The evolution of cyber-insurance industry and market: An institutional analysis. Telecommunications Policy, 44(8), 102007. doi: https://doi.org/10.1016/j.telpol.2020.102007

Lemnitzer, J. M. (2021). Why cybersecurity insurance should be regulated and compulsory. Journal of Cyber Policy, 1–19. doi: https://doi.org/10.1080/23738871.2021.1880609

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: Guided by information power. Qualitative Health Research, 26(13), 1753–1760. https://doi.org/10.1177/1049732315617444

Markopoulou, D. (2021). Cyber-insurance in EU policy-making: Regulatory options, the market's challenges and the US example. Computer Law & Security Review, 43, 105627. doi: https://doi.org/10.1016/j.clsr.2021.105627

Mott, G., Turner, S., Nurse, J. R. C., MacColl, J., Sullivan, J., Cartwright, A., & Cartwright, E. (2023). Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. Computers & Security, 128, 103162. doi: https://doi.org/10.1016/j.cose.2023.103162

Rangu, C. M., Badea, L., Scheau, M. C., Gabudeanu, L., Panait, I., Radu, V. (2024). Cyber insurance risk analysis framework considerations. Journal of Risk Finance, 25 (2), 224-252. doi: https://doi.org/10.1108/jrf-10-2023-0245

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. Information & Management, 59(4), 103638. doi: https://doi.org/10.1016/j.im.2022.103638

Schütz, F., Rampold, F., Kalisch, A., & Masuch, K. (2023). Consumer Cyber Insurance as Risk Transfer: A Coverage Analysis. Procedia Computer Science, 219, 521–528. doi: https://doi.org/10.1016/j.procs.2023.01.320

Wallace, S., Green, K. Y., Johnson, C. M., Cooper, J. T., & Gilstrap, C. M. (2020). An Extended TOE Framework for Cybersecurity Adoption Decisions. Communications of the Association for Information Systems, 47, 338–363. doi: https://doi.org/10.17705/1cais.04716

Wrede, D., Stegen, T., & Graf von der Schulenburg, J.-M. (2020). Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. The Geneva Papers on Risk and Insurance - Issues and Practice, 45(4), 657–689. doi: https://doi.org/10.1057/s41288-020-00183-6

Yeoh, W., Wang, S., Popovič, A., & Chowdhury, N. H. (2022). A systematic synthesis of critical success factors for cybersecurity. Computers & Security, 118, 102724. doi: https://doi.org/10.1016/j.cose.2022.102724

Zeller, G., & Scherer, M. A. (2020). A Comprehensive Model for Cyber Risk Based on Marked Point Processes and Its Application to Insurance. SSRN Electronic Journal. doi: https://doi.org/10.2139/ssrn.3668228