Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

INNOVATING TECHNOLOGY RISK MANAGEMENT AND CYBER RESILIENCE WITHIN THE CORPORATE SECTOR IN MALAYSIA

Ani Munirah Mohamad[1*]
Nur Syaedah Kamis[2]
Rohana Abdul Rahman[3]
Mazita Mohamed[4]
Norhayati Abdul Samat[5]

[1 – 5] School of Law, Universiti Utara Malaysia, Malaysia
*Corresponding Author: animunirah@uum.edu.my

Article history
Received date : 19-6-2026
Revised date : 20-6-2026
Accepted date : 25-7-2026
Published date : 1-8-2026

To cite this document:
Mohamad, A. M., Kamis, N. S., Abdul Rahman, R., Mohamed, M., & Abdul Samat, N. (2026). Innovating technology risk management and cyber resilience within the corporate sector in Malaysia. *International Journal of Accounting, Finance and Business (IJAFB),* 11 (67), 429 - 447.

Abstract: *The Malaysian corporate sector operates in an increasingly digitalised environment, expanding exposure to sophisticated cyber and technology risks. Despite the issuance of five key regulatory instruments, including those from Bank Negara Malaysia, the Securities Commission, Bursa Malaysia, NACSA, and MCMC, the regulatory landscape is characterized by a complex "multi-statute architecture" with significant fragmentation in legal character and prescriptive intensity. This study aims to map these five principal instruments, compare them across analytical dimensions such as risk management approaches and reporting mechanisms, and identify points of convergence and tension to propose innovative strategies. Utilizing a doctrinal legal research design supplemented by qualitative comparative analysis, the research reveals a universal shift from prevention to proactive cyber resilience and a shared emphasis on board-level oversight. However, critical tensions persist, particularly regarding uneven treatment of emerging technologies like artificial intelligence and conflicting incident reporting timelines, which range from same-day notification to unspecified periods. These discrepancies create a heavy compliance burden and hinder coordinated national responses. Key implications suggest the urgent need for a formal inter-regulator memorandum of understanding to harmonise reporting thresholds and align regulatory expectations. Additionally, the study recommends a unified cross-sectoral framework for emerging technologies and extended third-party oversight. By addressing these gaps, Malaysia can transition from its current fragmented regime toward a coherent, resilience-based governance landscape that better safeguards market integrity and national security against evolving digital threats.*

Keywords: *Technology risk management, cyber resilience, corporate sector, Innovation*

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

Introduction

The Malaysian corporate sector operates within an increasingly digitalised economic environment, in which reliance on cloud services, artificial intelligence, and interconnected information systems has become a defining feature of business operations. This shift has expanded productive capacity, yet it has also widened the surfaces through which organisations are exposed to technology and cyber risk (Pitafi & Awan, 2024). Data breaches, ransomware, distributed denial-of-service attacks, and third-party service disruptions now sit alongside conventional operational and financial risks on the corporate agenda, and boards of directors are progressively expected to integrate these exposures into enterprise risk management frameworks (Rahman et al., 2021; Rajola et al., 2025).

In response to the above-mentioned technological issues, five distinct instruments governing technology and cyber risk have been issued within the context of Malaysian corporate sectors. Bank Negara Malaysia's Risk Management in Technology (RMiT) policy document (current revision dated 28 November 2025); the Securities Commission Malaysia's Guidelines on Technology Risk Management (issued 1 August 2023, revised 19 August 2024); Bursa Malaysia's Guidance on Management of Cyber Risks (December 2022); the Cyber Security Act 2024 (Act 854), administered through the National Cyber Security Agency; and the MCMC MTSFB TC G009:2024 Technical Code registered on 4 April 2024. Together, these instruments signal a substantive expansion of the regulatory perimeter and align with a broader international movement from prevention-oriented postures toward resilience-based governance (AL-Hawamleh, 2024; Rajola et al., 2025).

Notwithstanding this expansion, closer examination reveals several unresolved concerns. First, the five instruments differ materially in legal character, sectoral coverage, and prescriptive intensity, ranging from criminal statute (the Cyber Security Act 2024) and binding prudential rules (BNM RMiT; SC Guidelines) to advisory guidance (Bursa) and registered technical code (MCMC). A single corporate group operating across financial services, listed markets, telecommunications, and designated national critical information infrastructure may fall within all five regimes simultaneously, generating compliance complexity that mirrors the fragmentation observed in other jurisdictions (Familoni & Shoetan, 2024; Oyeniyi et al., 2024). Second, treatment of emerging technologies is uneven: BNM RMiT and the SC Guidelines address artificial intelligence, machine learning, and cloud adoption in detail, while Bursa and MCMC engage these matters more sparsely, and the Cyber Security Act 2024 defers technical specification to sectoral codes of practice. Third, reporting timelines diverge, from same-day notification under the SC Guidelines to organisation-determined timing under the MCMC Technical Code, which complicates cross-regulator information sharing during a serious incident. Fourth, existing Malaysian scholarship has examined enterprise risk management, corporate governance, and risk disclosure largely as separate concerns (Khalik & Md. Sum, 2020; Kiflee & Ali Khan, 2021; Nasir & Hashim, 2020), and has not systematically compared the five technology and cyber risk instruments as a coherent regulatory landscape.

These gaps justify a comparative study to be carried out. Accordingly, this study pursues four objectives :

1. to map the five principal instruments governing technology and cyber risk in the Malaysian corporate sector;

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

2. to compare them across four analytical dimensions, namely the types of risks addressed, risk management approaches, reporting mechanisms, and innovative cyber-resilience strategies;
3. to identify convergent themes and points of tension, with particular attention to board centrality, treatment of emerging technologies, and cross-regulatory coordination; and
4. to propose recommendations for innovating technology risk management strategies in the Malaysian corporate sector.

Literature Review

The literature relevant to this paper falls into two connected fields: the international scholarship on cyber and technology risk governance, and the smaller but growing Malaysian legal scholarship. The review prioritises the latter, since the paper's focus is the Malaysian regulatory landscape. **Table 1** summarises the most salient contributions. Of Malaysian technology and cyber risk regulatory position.

Table 1. Selected literature on the Malaysian technology and cyber risk regulatory position, with international benchmarks

Study	Focus	Relevance to this paper
Sureani et al. (2021)	Adequacy of Malaysia's PDPA 2010, benchmarked against the UK Data Protection Act 2018	Identifies loopholes and enforcement gaps in the PDPA that intersect with data protection obligations across the five instruments
Sholehuddin et al. (2024)	Comparative personal data protection laws in Malaysia, Indonesia, Singapore, and the Philippines	Situates Malaysia within ASEAN and highlights differences in enforcement models
Ayub et al. (2024)	Malaysian legal position on search and seizure of digital evidence, compared with England and Wales	Documents statutory delay and fragmentation in Malaysian responses to the digital era
Daud et al. (2024)	Malaysian cybercrime response drawing on the Computer Crimes Act 1997, the Digital Signature Act 1997, the Electronic Commerce Act 2006, and the PDPA 2010	Confirms Malaysia's multi-statute, non-unified approach to cyber-related crime
Md Amin et al. (2023)	Blockchain in Malaysian banking under BNM and Securities Commission guidance	Illustrates how BNM and the Securities Commission coordinate on emerging technology risk while retaining separate mandates
Adanan et al. (2023); Sutan Maruhun et al. (2022)	Impact of the Malaysian Code on Corporate Governance (MCCG) 2000 to 2021 revisions on listed-issuer performance	Establishes the governance backdrop against which Bursa's Guidance on Management of Cyber Risks operates

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

Khalik and Md. Sum (2020)	Corporate governance and enterprise risk management (ERM) in Malaysian public listed companies	Board size significantly drives ERM implementation in Malaysian listed companies
Kiflee and Ali Khan (2021)	Risk disclosure practice in Malaysian listed companies	Notes a positive trend in overall risk disclosure but does not extend to technology or cyber risk categories
Hartmann and Carmenate (2021); Rajola et al. (2025)	International perspectives on board oversight of cyber risk and cyber resilience in the financial sector	Provide comparative benchmarks against which the Malaysian instruments can be assessed
Keskin et al. (2021)	Cyber third-party risk management	Third-party risk regulation remains globally at an early stage; a theme that also recurs across the Malaysian instruments

At the governance level, the Malaysian Code on Corporate Governance has been through five revisions since 2000, and provides the backdrop against which Bursa's Guidance on Management of Cyber Risks operates (Adanan et al., 2023; Sutan Maruhun et al., 2022). Empirical studies confirm that board attributes drive risk oversight and enterprise risk management implementation in Malaysian listed companies (Khalik & Md. Sum, 2020), yet risk disclosure practice remains uneven and has not systematically captured technology or cyber risk (Kiflee & Ali Khan, 2021). On emerging technologies, Md Amin et al. (2023) show that BNM and the Securities Commission coordinate through parallel guidance on blockchain and fintech, but without a unified inter-regulator framework. International scholarship on board oversight (Hartmann & Carmenate, 2021), cyber resilience in the financial sector (Rajola et al., 2025), and third-party cyber risk (Keskin et al., 2021) provides useful comparators but is not calibrated to the Malaysian statutory landscape.

Two gaps therefore emerge. First, no Malaysian study has systematically analysed the five principal technology and cyber risk instruments as a coherent whole, notwithstanding the well-documented tendency toward multi-statute fragmentation in Malaysian cyber-related law. Second, existing Malaysian scholarship on corporate governance and risk disclosure has not extended to technology or cyber risk specifically. This paper addresses both gaps by conducting a structured comparative analysis of BNM RMiT, the SC Guidelines, Bursa's Guidance, the Cyber Security Act 2024, and MCMC MTSFB TC G009:2024, thereby situating the Malaysian regime within the broader international discussion on innovating technology risk management.

Methodology

This study adopts a doctrinal legal research design supplemented by qualitative comparative analysis, which is the established approach for examining regulatory instruments in their statutory context. The primary sources comprise the five principal instruments governing technology and cyber risk in the Malaysian corporate sector, namely the Bank Negara Malaysia Risk Management in Technology policy document (2025 revision), the Securities Commission Guidelines on Technology Risk Management (2024 revision), Bursa Malaysia's Guidance on

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

Management of Cyber Risks (2022), the Cyber Security Act 2024, and the MCMC MTSFB TC G009:2024 Technical Code. Secondary sources include peer-reviewed literature retrieved through the academic database, together with relevant Malaysian legislation and regulatory guidance cited within the primary instruments.

The analysis proceeds in three stages. First, each instrument is mapped along four analytical dimensions: types of risks addressed, risk management approaches, reporting mechanisms, and innovative cyber-resilience strategies. Second, the instruments are compared across these dimensions to identify convergent themes and points of tension. Third, the findings are synthesised against the international literature to derive recommendations for innovating technology risk management strategies in the Malaysian corporate sector.

Analysis and Findings

This section deliberates on the analysis and findings of the study structured along the lines of the four objectives of the study.

Objective 1: Mapping and Description of the Five Regulatory Instruments on Technology Risk Management Within Corporate Sector in Malaysia

The first objective of this study is to map and describe the five principal instruments that govern technology and cyber risk in the Malaysian corporate sector. Each instrument is grounded in a distinct statutory or regulatory basis, targets a distinct population of entities, and carries a distinct legal weight. **Table 2** sets out their identifying features.

Table 2. Identification of the five Malaysian technology and cyber risk instruments

Feature	BNM RMiT	SC Guidelines on TRM	Bursa Guidance on Cyber Risks	Cyber Security Act 2024	MCMC MTSFB TC G009:2024
Issuing body	Bank Negara Malaysia	Securities Commission Malaysia	Bursa Malaysia Securities Berhad	National Cyber Security Agency (NACSA)	MCMC via Malaysian Technical Standards Forum Bhd
Legal nature	Mandatory policy document	Mandatory guidelines	Advisory best-practice guidance	Statute (Act 854) with criminal sanctions	Registered technical code (binding once registered)
Target entities	Licensed banks, insurers, takaful operators, e-money issuers, payment system operators	Capital market entities (brokers, fund managers, exchanges)	Public listed issuers	National Critical Information Infrastructure (NCII) entities across eleven sectors	Communications and multimedia organisations

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

Date of issue (current)	28 November 2025	1 August 2023 (revised 19 August 2024)	December 2022	Enacted 2024	Registered 4 April 2024
Sector coverage	Banking, insurance	Capital markets	Public listed companies	Cross-sectoral (eleven NCII sectors)	Telecommunications

Bank Negara Malaysia's Risk Management in Technology (RMiT) policy document, in its current revision dated 28 November 2025, is issued pursuant to Bank Negara Malaysia's supervisory powers under the Central Bank of Malaysia Act 2009, the Financial Services Act 2013, the Islamic Financial Services Act 2013, and cognate statutes governing money services businesses and payment systems. RMiT applies to licensed banks, insurers, takaful operators, e-money issuers, and payment system operators, and is binding on these institutions. Non-compliance may attract regulatory action under the enabling financial legislation.

The Securities Commission Malaysia's Guidelines on Technology Risk Management, issued on 1 August 2023 and revised on 19 August 2024, are made pursuant to section 377 of the Capital Markets and Services Act 2007. They apply to capital market entities including brokers, fund managers, and exchange operators, and are mandatory in nature. The Guidelines superseded the earlier Guidelines on Management of Cyber Risk that the SC had issued in 2016, and represent a substantive broadening from cyber risk narrowly to technology risk more generally.

Bursa Malaysia Securities Berhad issued its Guidance on Management of Cyber Risks in December 2022 as a best-practice document for listed issuers. Unlike RMiT and the SC Guidelines, Bursa's Guidance is advisory rather than binding, and it operates alongside rather than within the Main Market and ACE Market Listing Requirements. Its influence derives from its status as a supplement to the Malaysian Code on Corporate Governance framework governing listed-issuer conduct.

The Cyber Security Act 2024 (Act 854), administered through the National Cyber Security Agency (NACSA), is a statute rather than subsidiary regulation, and carries criminal sanctions on conviction. It applies to entities designated as national critical information infrastructure (NCII) entities across eleven sectors: government, banking and finance, transportation, defence and national security, information, communication and digital, healthcare services, water, sewerage and waste management, energy, agriculture and plantation, trade, industry and economy, and science, technology and innovation. Sector leads are appointed by the Minister and are empowered to designate the NCII entities within their sectors.

The Malaysian Communications and Multimedia Commission (MCMC), acting through the Malaysian Technical Standards Forum Bhd, registered the Technical Code MCMC MTSFB TC G009:2024 (Second Revision) on 4 April 2024, under section 185 of the Communications and Multimedia Act 1998. The Technical Code becomes binding on communications and multimedia organisations once registered. It aligns with ISO/IEC 27001 and complements

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

companion codes on the Malaysia Critical Security Controls (TC G042), monitoring and measurement of security control objectives (TC G021), and cognate technical matters. The five instruments therefore span the principal economic sectors of the Malaysian corporate sector, though they arise from different legal bases and carry different degrees of legal weight.

Objective 2: Comparative Analysis Across Four Dimensions

The second objective is to compare the five instruments across four analytical dimensions: types of risks addressed, risk management approaches, reporting mechanisms, and innovative cyber-resilience strategies. This subsection presents the comparison one dimension at a time.

Types of Risks Addressed

BNM RMiT casts the widest net. Its risk taxonomy captures distributed denial-of-service attacks, data loss in motion and at rest, customer information breach, cyber supply chain risks, third-party concentration risk, geopolitical risk, cloud risk, emerging technology risk, and shadow IT. The breadth is consistent with the prudential function of the central bank, which is concerned not only with the individual institution's operational continuity but also with the systemic stability of the financial system as a whole. Cyber supply chain risk, in particular, has emerged as a recognised systemic exposure in the international literature (Keskin et al., 2021), and BNM RMiT's explicit inclusion of fourth-party considerations places Malaysia among the more forward-looking jurisdictions on this dimension.

The SC Guidelines emphasise technology incidents, cyber incidents, and near-miss events, together with risks arising from the adoption of artificial intelligence and machine learning. Under Appendix 3 of the Guidelines, capital market entities must observe principles of accountability, transparency, fairness, and practical accuracy and reliability when deploying AI and ML systems. The near-miss category is analytically important because it captures events that did not materialise into loss but revealed vulnerabilities, thereby extending the risk universe beyond consummated incidents.

Bursa's Guidance addresses security risk (data loss, identity theft, identity fraud, cyber threats, and unauthorised physical access), together with the financial, operational, and reputational consequences that flow from a materialised event. The framing is consistent with Bursa's role as the securities exchange, which is concerned with the integrity and orderliness of the market rather than the systemic prudential stability of any individual issuer.

The Cyber Security Act 2024 frames cyber threats and incidents against NCII as a national security concern. Section 5 of the Act defines cyber security as the state in which a computer or computer system is protected from any attack or unauthorised access such that it continues to be available and operational and its integrity and confidentiality are maintained. The statutory language deliberately elevates cyber risk from an enterprise concern to a public-interest one, reflecting the shift toward treating certain digital infrastructures as national assets.

The MCMC Technical Code, being ISO-aligned, addresses threats to the confidentiality, integrity, and availability of information assets at a generic level. Its risk framing is drawn from ISO/IEC 27001 and applies without material adaptation to the sector context.

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

The instruments therefore differ not only in the coverage of their risk taxonomies but in the underlying risk conceptualisation: enterprise and systemic risk (BNM), market integrity and investor protection (SC), strategic and reputational risk (Bursa), national security and public interest (NACSA), and operational and standards-compliance risk (MCMC). These differences are not merely rhetorical: they shape the calibration of controls, the design of reporting mechanisms, and the degree of prescriptive intensity that each instrument imposes.

Risk Management Approaches

The following **Table 3** summarises the required framework, governance structure, operational controls, and third-party oversight expectations across the five instruments.

The prescriptive intensity descends from BNM RMiT at the most detailed end, through the SC Guidelines and the Cyber Security Act 2024 in the middle, to Bursa's Guidance and the MCMC Technical Code at the more principles-based end. BNM RMiT uniquely requires two frameworks rather than one: a Technology Risk Management Framework (TRMF) and a separate Cyber Resilience Framework (CRF). The rationale is that technology risk (encompassing hardware, software, operational, and third-party dimensions) and cyber risk (encompassing intentional adversarial threats) are conceptually distinct even if they overlap operationally. The SC Guidelines, by contrast, integrate technology and cyber risk within a single TRM Framework covering five domains: technology risk management, technology operations management, technology service provider management, cyber security management, and AI and ML principles.

Bursa's Guidance requires the integration of cyber risk into the listed issuer's overall enterprise risk management framework rather than the establishment of a separate framework, consistent with its non-binding character. The Cyber Security Act 2024 delegates the framework function to sectoral Codes of Practice prepared by sector leads and endorsed by the Chief Executive of NACSA. The MCMC Technical Code prescribes an Information and Network Security management system aligned with ISO/IEC 27001, with the ISO framework serving as the operational template

Table 3. Comparison of risk management approaches

Element	BNM RMiT	SC Guidelines	Bursa Guidance	Cyber Security Act 2024	MCMC TC G009
Required framework	Technology Risk Management Framework and separate Cyber Resilience Framework	TRM Framework covering five domains including AI and ML principles	Cyber risk management framework integrated into overall ERM	Sectoral Code of Practice prepared by sector lead	Information and Network Security management system aligned with ISO/IEC 27001
Governance structure	Board approves risk appetite; designated	Board oversight with designated	Board as apex governing body; senior	Sector leads appointed by	Leadership and commitment from top

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

	board-level committee with at least one tech-competent member; CISO required	senior management responsible person	management responsible person	Minister; NCII entities designated by sector leads	management; CISO referenced
Operational controls	Highly prescriptive (encryption, DLP, DDoS mitigation, penetration testing, environment segregation)	Prescriptive (compromise assessments, annual penetration testing, baseline security configuration)	Principles-based (anti-virus, firewalls, penetration testing, awareness training)	Determined by sectoral code; mandatory risk assessment and audit	Aligned with Malaysia Critical Security Controls and ISO 27001 controls
Third-party oversight	Detailed (due diligence, contractual terms, monitoring, fourth-party considerations)	Required (due diligence, contract management, periodic assessment)	General (include third parties in awareness, testing, and policies)	Cyber security service providers must be licensed under the Act	Generic ISO-aligned supplier relationship management
Audit requirements	Independent technology audit function under Board Audit Committee; external assurance for digital service launches	Independent assessment; internal audit involvement	Internal audit oversight; periodic testing of cyber resilience framework	Mandatory audit by NACSA-approved auditor; report within 30 days of completion	Internal audits and management review per ISO management system

On governance, all five instruments place the board of directors at the apex of oversight, consistent with the international literature that has documented the shift from board passivity to substantive board engagement in cyber risk oversight (Hartmann & Carmenate, 2021; Rahman et al., 2021). BNM RMiT is the most prescriptive, requiring a designated board-level committee with at least one member possessing technology experience and competencies, and mandating the designation of a Chief Information Security Officer (CISO) who must be independent from day-to-day technology operations, appropriately certified, and empowered with sufficient authority and resources. The SC Guidelines require board oversight and designated senior management, but do not mandate a technology-competent board member. Bursa's Guidance identifies the board as the apex governing body and requires the identification of a senior management responsible person, but again without the technology-competence

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

requirement. The Cyber Security Act 2024 approaches governance through the sector lead and Chief Executive of NACSA rather than through the entity's own board, while the MCMC Technical Code invokes the ISO concept of leadership and top-management commitment and references the CISO role.

On operational controls, BNM RMiT is again the most detailed, with prescriptive requirements on encryption, data loss prevention, DDoS mitigation, penetration testing, vulnerability assessment, and environment segregation. The SC Guidelines require compromise assessments, annual penetration testing, baseline security configurations, and behavioural analytics for signature-less malware detection. Bursa's Guidance is principles-based, referencing anti-virus, firewalls, penetration testing, monitoring, and awareness training without detailed prescription. The Cyber Security Act 2024 leaves operational specifics to sectoral Codes of Practice and requires mandatory risk assessment and audit at intervals prescribed by regulation. The MCMC Technical Code aligns with the Malaysia Critical Security Controls (MyCSC) and ISO 27001 controls.

On third-party oversight, BNM RMiT is again the most sophisticated, with detailed provisions on due diligence, contractual terms, monitoring, and supply chain risk management, including explicit consideration of fourth parties (that is, the third parties of the entity's own third parties). The SC Guidelines require due diligence, contract management, and periodic capability assessment. Bursa's Guidance addresses third parties generally, requiring their inclusion in awareness, testing, and policies. The Cyber Security Act 2024 introduces a distinctive innovation: cyber security service providers must be licensed under the Act, thereby placing third-party providers within a regulatory perimeter of their own. The MCMC Technical Code applies generic ISO-aligned supplier relationship management.

Reporting Mechanisms

Reporting mechanisms are the third dimension of comparison. **Table 4** summarises the reporting channel, incident timeline, pre-implementation notification, and penalty for non-reporting. Four substantive observations emerge.

Table 4. Comparison of reporting mechanisms

Element	BNM RMiT	SC Guidelines	Bursa Guidance	Cyber Security Act 2024	MCMC TC G009
Reporting channel	BNM (notifications and consultations)	SC Vault system (primary); email backup	Internal escalation to board; no statutory external channel	Chief Executive of NACSA and relevant sector lead	Internal documentation; separate CMA 1998 reporting
Incident timeline	Timely escalation per Cyber Incident	On the day of detection for any technology,	No fixed external timeline	Within a period prescribed by	Per organisation's documented procedure

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

	Response Plan	cyber, or near-miss event		subsidiary regulations	
Pre-implementation notification	Required for new digital services and first-time public cloud adoption for critical systems	Required for major technology-related implementations	Not required	Material changes to NCII must be notified	Not specified
Penalty for non-reporting	Regulatory action under Financial Services Act	Regulatory action under Capital Markets and Services Act	No direct penalty	Fine up to RM500,000 or imprisonment up to ten years, or both (section 23)	Indirect enforcement under the Communications and Multimedia Act 1998
Required report content	Risk assessment, security arrangements, terms, client charter, privacy policy, outsourcing arrangements	Contact details, incident type, time, description, system impact, geographic and IP details, resolution actions	Not formally prescribed	Per directives and code of practice; situational reports from sector lead to Chief Executive	Per organisation's documented procedure

First, the reporting channels are institutionally distinct. BNM operates through its supervisory relationship with regulated financial institutions, receiving notifications and consultations directly. The SC operates through the SC Vault system as the primary channel, with email backup. Bursa relies on internal escalation from senior management to the board of the listed issuer, without a statutory external channel. NACSA receives reports from the sector lead, which in turn receives notifications from NCII entities. The MCMC Technical Code leaves external reporting to be handled under the Communications and Multimedia Act 1998, treating the Technical Code itself as internal documentation.

Second, the incident timelines diverge considerably. The SC's requirement to notify on the day of detection for any technology incident, cyber incident, or near-miss event is the most stringent by clock time. BNM RMiT requires timely escalation within the parameters of the entity's Cyber Incident Response Plan, which typically prescribes short internal timelines but is entity-specific rather than uniform. Bursa imposes no fixed external timeline. The Cyber Security Act 2024 leaves the notification period to be prescribed by subsidiary regulations, which as at the time of writing had not been finalised. The MCMC Technical Code defers timing to the

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

organisation's documented procedure. These divergent timelines have practical consequences: a single incident affecting a listed financial institution that is also an NCII entity would trigger multiple reporting obligations with different clocks running simultaneously.

Third, pre-implementation notification is required by BNM (for new digital services and first-time public cloud adoption for critical systems) and by the SC (for major technology-related implementations affecting business or clients). The Cyber Security Act 2024 requires notification of material changes to NCII. Bursa's Guidance and the MCMC Technical Code do not require pre-implementation notification. The presence or absence of ex ante scrutiny is a meaningful design choice, since it enables the regulator to review the risk implications of a proposed implementation before rather than after deployment.

Fourth, the penalties for non-reporting differ sharply. BNM and the SC can invoke regulatory action under the Financial Services Act and the Capital Markets and Services Act respectively. Bursa imposes no direct penalty, though non-compliance may be addressed through the Listing Requirements separately. The Cyber Security Act 2024 carries the most severe sanction: a fine of up to RM500,000 or imprisonment of up to ten years, or both, under section 23. The MCMC Technical Code carries no direct penalty but may be enforced indirectly under the Communications and Multimedia Act 1998. The intensity of the sanction shapes the compliance calculus, and the criminal law posture of the Cyber Security Act 2024 marks a notable escalation in Malaysian cyber-related legal enforcement.

Innovative Cyber-Resilience Strategies

The fourth dimension concerns the innovative strategies each instrument advances for cyber resilience. **Table 5** summarises the resilience model, innovative features, testing and exercises, learning mechanisms, and capacity-building expectations.

BNM RMiT operationalises the identify-protect-detect-respond-recover (IPDRR) model borrowed from the NIST Cybersecurity Framework, and its Cyber Resilience Framework is specifically directed at ensuring operational resilience against extreme but plausible cyber-attacks. The introduction of contemporary features distinguishes BNM RMiT within the Malaysian regulatory landscape: Software Bill of Materials (which is a machine-readable inventory of components used in software), infrastructure-as-code (which treats infrastructure configuration as versioned software), immutable infrastructure (where servers are replaced rather than reconfigured), federated identity management for cloud services, dark web monitoring for compromised credentials, a multi-cloud strategy to reduce concentration risk, and cyber threat intelligence integration. These features reflect contemporary cybersecurity practice at the international frontier and correspond to what Rajola et al. (2025) describe as the shift from purely preventive measures toward proactive response and recovery.

The SC Guidelines apply a cyber security lifecycle of preparation, detection and analysis, containment and recovery, and post-incident review. Their most distinctive innovation is the ethical AI framework in Appendix 3, which prescribes four principles: accountability, transparency and explainability, fairness and non-discrimination, and practical accuracy and reliability. The behavioural analytics requirement for signature-less malware detection is likewise a contemporary feature, reflecting the recognition that pattern-matching against known signatures is no longer sufficient given adversarial adaptation.

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

Table 5. Comparison of innovative cyber-resilience strategies

Element	BNM RMiT	SC Guidelines	Bursa Guidance	Cyber Security Act 2024
Resilience model	IPDRR (identify, protect, detect, respond, recover); operational resilience against extreme but plausible attacks	Cyber security lifecycle (preparation, detection and analysis, containment and recovery, post-incident review)	Anticipate, absorb, adapt, respond, recover cycle	National coordination via National Cyber Coordination and Command Centre System
Innovative features	Software Bill of Materials, infrastructure-as-code, immutable infrastructure, federated identity management, dark web monitoring, multi-cloud strategy, cyber threat intelligence	Ethical AI principles (accountability, transparency, fairness, reliability); behavioural analytics for signature-less malware detection	Cultural emphasis: random staff testing, security culture across people-process-technology, predictive capabilities	Centralised national cyber command centre; mandatory cyber security exercises; licensing regime for cyber security service providers
Testing and exercises	Vulnerability assessment, penetration testing, integrated business continuity and cyber drills with cloud providers	Annual penetration testing; compromise assessments on critical systems	Periodic testing of cyber resilience framework including third parties; scenario simulations	Cyber security exercises conducted by NACSA on NCII entities
Learning mechanism	Post-incident review; key performance indicators; regular board updates	Post-incident review reports to relevant stakeholders; cyber threat intelligence integration	Distil lessons from global and local incidents; continuous improvement of detection capabilities	Investigation by authorised officer; lessons fed into sectoral codes
Capacity building	Mandatory cybersecurity awareness training; CISO competency; cross-functional committee	Workforce capability for AI and ML; cyber awareness; competency of senior management	Enterprise-wide awareness and education for board, employees and third parties; random testing	Cyber security expert appointments; licensing creates a regulated profession

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

Bursa's Guidance follows an anticipate-absorb-adapt-respond-recover cycle drawn from the cyber resilience literature. Its distinctive contribution is cultural: it emphasises random staff testing to measure the effectiveness of awareness training, promotes a security culture that spans people, processes, and technology, and advocates the development of predictive capabilities. It also explicitly recognises that cyber resilience extends beyond the information technology environment and requires proactive engagement between IT, senior management, and the board.

The Cyber Security Act 2024 introduces two national-level innovations. The National Cyber Coordination and Command Centre System provides a centralised architecture for information sharing and coordinated response during a serious cyber incident. Mandatory cyber security exercises, or drills, are provided for under section 24, giving the Chief Executive of NACSA the power to test the preparedness of NCII entities. The licensing regime for cyber security service providers under Part VI establishes a regulated profession, potentially raising baseline competence and accountability across the ecosystem.

The MCMC Technical Code applies the ISO Plan-Do-Check-Act cycle for continual improvement, and its most distinctive innovation is its harmonisation with international standards including ISO, NIST, CIS, and ITU-T. The modular technical code architecture, whereby TC G009 is complemented by companion codes on IoT, 5G, cloud, and privacy information management, permits calibrated adaptation to specific technology domains without amending the general framework.

Taken together, the innovative features across the five instruments reveal a Malaysian regulatory landscape that is broadly consistent with international good practice, though the depth of innovation is unevenly distributed. BNM RMiT and the Cyber Security Act 2024 sit at the frontier; the SC Guidelines are strong on AI governance; Bursa's cultural emphasis is analytically valuable but principles-based; and the MCMC Technical Code is standards-anchored rather than innovation-driven.

Objective 3: Convergent Themes and Points of Tension

The third objective is to identify the convergent themes and points of tension across the five frameworks. Both are equally important: convergence points to the maturing of a shared regulatory logic, while tensions point to the areas requiring further coordination or reform.

Convergent Themes

Three convergent themes emerge from the comparative analysis. First, board centrality is universal across the five instruments. Every instrument places the board of directors at the apex of technology and cyber risk governance, whether by requiring board approval of risk appetite (BNM RMiT, SC Guidelines), designating the board as the apex governing body (Bursa Guidance), embedding board oversight through sector leads and the Chief Executive of NACSA (Cyber Security Act 2024), or invoking top-management commitment (MCMC Technical Code). This convergence reflects a broader international consensus that cyber risk oversight is a board-level responsibility that cannot be delegated wholly to the information technology function (Hartmann & Carmenate, 2021; Rahman et al., 2021). Within Malaysia, this expectation is reinforced by the Malaysian Code on Corporate Governance, most recently

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

revised in 2021, which frames the board as the apex risk governance body for listed companies (Adanan et al., 2023; Sutan Maruhun et al., 2022)..

Second, all five instruments have moved away from prevention-only thinking toward resilience-based governance. This is evident in BNM RMiT's separate Cyber Resilience Framework, the SC's cyber security lifecycle, Bursa's anticipate-absorb-adapt-respond-recover model, the Cyber Security Act 2024's national coordination architecture, and the MCMC Technical Code's continual improvement mandate. The shift is significant because it acknowledges that some cyber-attacks will succeed despite preventive controls, and that the measure of good governance is therefore the capacity to respond and recover rather than the mere presence of preventive controls. The international literature has documented the same shift in comparative jurisdictions (Rajola et al., 2025; AL-Hawamleh, 2024).

Third, third-party and supply chain exposure is recognised across the instruments, though with varying depth. BNM RMiT's fourth-party considerations sit at one end of the spectrum, addressing the sub-contractors of the entity's own service providers. The SC Guidelines require due diligence and periodic assessment of third-party providers. Bursa's Guidance includes third parties in awareness and testing programmes. The Cyber Security Act 2024 introduces a licensing regime for cyber security service providers. The MCMC Technical Code applies ISO-aligned supplier relationship management. The recognition of third-party risk as a first-order concern across all five instruments is consistent with the international literature (Keskin et al., 2021), which has identified third parties as a principal attack vector in recent year).

Points of Tension

The study identified four points of tension to be equally clear. First, prescription and flexibility pull against each other across the instruments. BNM RMiT and the SC Guidelines are highly prescriptive, providing detailed technical requirements that leave limited discretion. Bursa's Guidance is principles-based, permitting adaptation to the listed issuer's specific risk profile. The MCMC Technical Code adopts an ISO management-system approach, which is procedural rather than technical in nature. The Cyber Security Act 2024 defers technical detail to sectoral Codes of Practice yet imposes the most severe criminal penalty for non-compliance. A single corporate group operating across sectors may therefore be simultaneously subject to a prescriptive regime (from BNM), a principles-based regime (from Bursa), and a criminal-law regime (under the Cyber Security Act 2024), each of which employs a different regulatory logic..

Second, the treatment of emerging technologies is uneven. BNM RMiT and the SC Guidelines address AI, machine learning, and cloud adoption in detail. Bursa's Guidance references emerging technology risk in principles-based terms. The Cyber Security Act 2024 defers technical detail to sectoral Codes of Practice, meaning the treatment of any specific emerging technology depends on the sector to which the NCII entity belongs. The MCMC Technical Code addresses emerging technology through companion technical codes on IoT, 5G, and cloud. The unevenness raises a concern about regulatory coverage: a listed company that adopts AI outside the financial sector may face weaker guidance than a bank adopting the same technology, notwithstanding that the underlying risk may be substantively identical..

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

Third, reporting timelines diverge from same-day (SC) to unspecified (MCMC). This divergence complicates cross-regulator information sharing during a serious incident and may impede the coordinated national response that the Cyber Security Act 2024 was intended to enable. It also creates compliance complexity for corporate risk officers, who must reconcile multiple reporting clocks in the immediate aftermath of an incident when decisive action is most needed..

Fourth, cross-regulatory coordination gaps arise where a single corporate group falls within multiple regimes simultaneously without a formal inter-regulator mechanism to reconcile potentially divergent requirements. The SC Guidelines at paragraph 3.03 acknowledge this issue for jointly regulated entities and provide that where requirements differ, the more stringent requirement shall apply. However, no equivalent provision exists across the other four instruments, and there is no formal Malaysian analogue to the inter-agency coordination mechanisms observed in other jurisdictions (Familoni & Shoetan, 2024; Malatji et al., 2020).

Objective 4: Recommendations for Innovating Technology Risk Management Strategies Within the Corporate Sectors in Malaysia

The fourth objective is to propose recommendations for innovating technology risk management strategies in the Malaysian corporate sector. Four recommendations are advanced, each supported by the comparative findings above and calibrated to the Malaysian regulatory context.

First, a Malaysian inter-regulator memorandum of understanding covering BNM, the SC, Bursa, NACSA, and MCMC would provide a formal coordination architecture for reconciling overlapping obligations, aligning reporting thresholds where practicable, and sharing incident intelligence during a serious cyber event. Such an instrument could adopt as its point of departure the SC Guidelines' principle that where jointly regulated entities face differing requirements, the more stringent requirement shall apply. It could go further by designating a lead regulator for corporate groups that straddle multiple regimes, thereby reducing compliance complexity without diluting substantive requirements. The National Cyber Coordination and Command Centre System established by the Cyber Security Act 2024 provides a natural institutional locus for the coordination function.

Second, the treatment of emerging technologies should be harmonised through a Malaysian AI, cloud, and emerging-technology principles document jointly issued by the five regulators. The SC Guidelines' four AI principles (accountability, transparency and explainability, fairness and non-discrimination, and practical accuracy and reliability) are analytically strong and could be adapted for cross-sectoral use. BNM RMiT's detailed cloud provisions could be similarly generalised, subject to appropriate calibration for the sensitivity of the sector.

Third, reporting mechanisms should be aligned around a common minimum standard, such as notification within twenty-four hours of detection, calibrated to the differing risk profiles of each sector. The SC's same-day standard is the appropriate benchmark for the financial sector; a slightly longer period may be justified for less time-sensitive sectors provided the aggregate national picture can be assembled promptly. Alignment need not require identity of timelines but should require compatibility of clocks, so that a single incident affecting entities in multiple sectors can be reported into a common repository within a compressed window.

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

Fourth, third-party and supply chain oversight should be extended beyond the financial sector by mainstreaming BNM's fourth-party considerations and the Cyber Security Act 2024's licensing regime for cyber security service providers into a whole-of-corporate-sector expectation. Public listed companies and communications entities should be subject to comparable third-party oversight standards, particularly where they rely on the same cloud service providers, managed security service providers, and software vendors that already fall within the BNM perimeter. This would address the international observation that third-party risk regulation remains at an early stage of development (Keskin et al., 2021) by giving Malaysia a coherent national response.

Taken together, these recommendations situate the Malaysian regime as a working example of how an emerging economy may transition from a fragmented multi-instrument architecture toward a coherent, resilience-based technology risk management landscape. The recommendations are calibrated to be implementable within the existing legal structure, without requiring new primary legislation, and can be pursued incrementally through regulatory coordination, joint guidance, and administrative agreement.

Conclusion

The analysis of cyber resilience governance in the Malaysian corporate sector reveals a complex multi-statute architecture that elevates cyber risk to a board-level priority but introduces significant compliance challenges. While there is a universal shift toward proactive, resilience-based governance—best exemplified by Bank Negara Malaysia's IPDRR model and the Cyber Security Act 2024—fragmentation across five regulatory instruments creates a heavy burden for cross-sectoral entities. This is most visible in conflicting incident reporting timelines, ranging from the Securities Commission's same-day requirement to unspecified periods in other sectors. Furthermore, the treatment of emerging technologies like AI is unevenly distributed, with robust frameworks from BNM and the SC contrasting with more principles-based approaches elsewhere. In conclusion, while Malaysia has established a foundation for cyber risk management, the landscape remains siloed and lacks a unified inter-regulator framework. The transition from a patchwork of statutes to a coherent, resilience-based regime is necessary to protect critical infrastructure. By addressing identified tensions through formal coordination and harmonized technical standards, Malaysia can better safeguard market integrity against increasingly sophisticated digital threats.

The implications of this study suggest a path toward regulatory maturity. Policy-wise, there is an urgent need for an inter-regulator memorandum of understanding to align reporting thresholds and reconcile overlapping obligations. Managerially, boards must include members with technology competencies, as delegating cyber risk solely to IT departments is no longer sufficient under current expectations. Finally, regulators should develop a cross-sectoral harmonized principles document for AI and cloud adoption to ensure consistent security standards across all industries, preventing gaps where underlying technology risks are identical.

Acknowledgements

The authors would like to acknowledge and extend a special appreciation to Universiti Utara Malaysia for financially supporting this work through the Research Group initiative.

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

References

Adanan, S. A., Saidin, A., & Bustamam, K. S. (2023). The effect of gender diversity and board independence on firms performance. International Journal of Academic Research in Business and Social Sciences, 13(10). https://doi.org/10.6007/ijarbss/v13-i10/19007

AL-Hawamleh, A. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. International Journal of Computing and Digital Systems, 15(1), 1315–1331. https://doi.org/10.12785/ijcds/150193

Ayub, Z. A., Labanieh, M. F., & Abdul Wahab, H. (2024). A legislative analysis of Malaysian legal system on search and seizure procedure of digital evidence. In Proceedings of the international conference (pp. 259–270). Atlantis Press International BV. https://doi.org/10.2991/978-94-6463-352-8_20

Daud, P., Muniandy, N. A. L., & Nadi, F. (2024). Publics perception and awareness towards the identity theft among the residents of Bistari Impian Apartment, Johor, Malaysia. International Journal of Academic Research in Business and Social Sciences, 14(11). https://doi.org/10.6007/ijarbss/v14-i11/23385

Familoni, B. T., & Shoetan, P. O. (2024). Cybersecurity in the financial sector: A comparative analysis of the USA and Nigeria. Computer Science & IT Research Journal, 5(4), 850–877. https://doi.org/10.51594/csitrj.v5i4.1046

Hartmann, C., & Carmenate, J. (2021). Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: Implications for practice, policy, and research. Current Issues in Auditing, 15(2), A9–A23. https://doi.org/10.2308/ciia-2020-034

Keskin, O. F., Caramancion, K. M., & Tatar, I. (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. Electronics, 10(10), 1168. https://doi.org/10.3390/electronics10101168

Khalik, Z. A., & Md. Sum, R. (2020). The influence of corporate governance on enterprise risk management implementation: A study on non-financial public listed companies in Malaysia. Journal of Technology Management and Business, 7(1). https://doi.org/10.30880/jtmb.2020.07.01.005

Kiflee, A. K. R., & Ali Khan, M. N. A. (2021). The effect of performance and corporate governance to risk disclosure among listed companies in Malaysia. Asia-Pacific Management Accounting Journal, 16(1), 119–161. https://doi.org/10.24191/apmaj.v16i1-06

Malatji, M., Marnewick, A. L., & von Solms, S. (2020). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. Sustainability, 13(1), 291. https://doi.org/10.3390/su13010291

Md Amin, W. L., Mat Ali, S. A., & Mat Ali, S. A. (2023). Blockchain technology a structural shifts in banking sector: Consumer-oriented measures. International Journal of Academic Research in Accounting, Finance and Management Sciences, 13(2). https://doi.org/10.6007/ijarafms/v13-i2/18019

Nasir, N. A. M., & Hashim, H. A. (2020). Corporate governance performance and financial statement fraud: Evidence from Malaysia. Journal of Financial Crime, 28(3), 797–809. https://doi.org/10.1108/jfc-09-2020-0182

Oyeniyi, L. D., Ugochukwu, C. E., & Mhlongo, N. Z. (2024). Developing cybersecurity frameworks for financial institutions: A comprehensive review and best practices. Computer Science & IT Research Journal, 5(4), 903–925. https://doi.org/10.51594/csitrj.v5i4.1049

Volume: 11 Issues: 67 Special Issue [August, 2026] pp. 429 - 447
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.academicinspired.com/ijafb
DOI: 10.55573/IJAFB.116728

Pitafi, Z. R., & Awan, T. M. (2024). Cybersecurity and risk management: New frontiers in corporate governance. IntechOpen. https://doi.org/10.5772/intechopen.1005153

Rahman, M. B., Karim, T., & Chowdhury, I. U. (2021). Role of boards in cybersecurity risk profiling: The case of Bangladeshi commercial banks. Global Journal of Management and Business Research, 21(3), 49–58. https://doi.org/10.34257/gjmbravol21is3pg49

Rajola, F., Gatelli, P., & Iacopino, V. (2025). Governance processes and technologies for cyber resilience in the financial sector: The Italian scenario. Information Systems Journal, 36(4), 582–596. https://doi.org/10.1111/isj.70023

Sholehuddin, N., Miskam, S., & Mohd Shahwahid, F. (2024). A comparative legal analysis on personal data protection laws in selected ASEAN countries. Journal of Muwafaqat, 7(1), 23–38. https://doi.org/10.53840/muwafaqat.v7i1.166

Sureani, N. B. N., Awis Qurni, A. S. B., & Azman, A. H. B. (2021). The adequacy of data protection laws in protecting personal data in Malaysia. Malaysian Journal of Social Sciences and Humanities, 6(10), 488–495. https://doi.org/10.47405/mjssh.v6i10.1087

Sutan Maruhun, E. N., Mohd Azmi, A. N., & Mohd Shaari, S. N. (2022). Impact of corporate governance on firm performance of Malaysian public listed construction firms during COVID-19 pandemic. International Journal of Academic Research in Business and Social Sciences, 12(11). https://doi.org/10.6007/ijarbss/v12-i11/15095.