



## SUSTAINABILITY RISK MANAGEMENT AND INFORMATION TECHNOLOGY GOVERNANCE IN MALAYSIA

Wan Norhayati Wan Ahmad<sup>1\*</sup>, Azharudin Ali<sup>2</sup>, Ani Munirah Mohamad<sup>3</sup>, Mohd Zakhiri Md Nor<sup>4</sup>

- <sup>1</sup> Tunku Puteri Intan Safinaz School of Accountancy (TISSA) and Institute for Strategic and Sustainable Accounting Development (ISSAD), Universiti Utara Malaysia (UUM), Malaysia  
Email: [wnwa@uum.edu.my](mailto:wnwa@uum.edu.my)
  - <sup>2</sup> Tunku Puteri Intan Safinaz School of Accountancy (TISSA) and Institute for Strategic and Sustainable Accounting Development (ISSAD), Universiti Utara Malaysia (UUM), Malaysia  
Email: [azharudin@uum.edu.my](mailto:azharudin@uum.edu.my)
  - <sup>3</sup> School of Law and Centre for Testing, Measurement and Appraisal (CeTMA), Universiti Utara Malaysia (UUM), Malaysia  
Email: [animunirah@uum.edu.my](mailto:animunirah@uum.edu.my)
  - <sup>4</sup> School of Law and Legal and Justice Research Centre (LJRC), Universiti Utara Malaysia (UUM), Malaysia  
Email: [zakhiri@uum.edu.my](mailto:zakhiri@uum.edu.my)
- \* Corresponding Author

### Article Info:

#### Article history:

Received date: 27.12.2021  
Revised date: 07.02.2022  
Accepted date: 20.02.2022  
Published date: 07.03.2022

#### To cite this document:

Wan Ahmad, W. N., Ali, A., Mohamad, A. M., Md Nor, M. Z. (2021). Sustainability Risk Management and IT Governance in Malaysia. *Journal of Information System and Technology Management*, 7 (25), 54-64.

DOI: 10.35631/JISTM.725004

This work is licensed under [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/)



### Abstract:

Sustainability encompasses more than green and environmental protection. That is why the United Nations' sustainable development goals (SDGs) comprise 17 targets aimed at achieving global sustainability through shared prosperity and peace for people and the planet, both at present and in the future. SDG-9, which focuses on resilient infrastructure, sustainable industrialisation, and innovation, calls for investment in information technology (IT) to support sustainable development and community empowerment. Regardless of the amount to which IT can assist in accomplishing goals, it requires adequate control. Otherwise, it will exacerbate threats to the environment and society, as well as to the corporate organisation. IT governance is primarily motivated by the need for an organisation's risks to be transparent and its stakeholder values to be protected. By contrast, sustainable risk management (SRM) is a systematic strategy to managing an organisation's environmental, social, and governance risks (ESG). This conceptual paper discusses the function of information technology governance and its effect on the practise of SRM in Malaysia. The study highlights four IT governance functions that have an impact on sustainability risks: protection against reputational risk, guaranteeing equal access, reducing environmental impact, mitigation of online fraud and improper business, and protecting data integrity and confidentiality. This study would shed light on the sustainability hazards associated with information technology and raise awareness of their influence on society and the environment. As a result, it is envisaged that the objectives for IT investment are met while also mitigating IT risks. Hopefully, this study can serve as a stimulus for further research on related topics of IT governance

and sustainable risk management on a worldwide scale, and particularly in the Malaysian context.

**Keywords:**

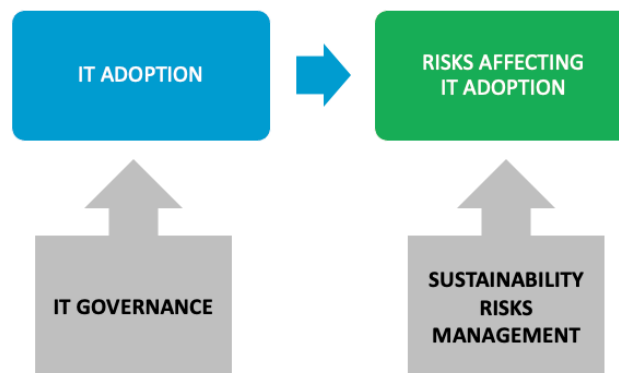
Sustainable Risk Management, IT Governance, SDG-9, Sustainable Development Goals

## Introduction

Information technology (IT) is critical to the survival of businesses, particularly in terms of increasing organisational communication and coordinating work-related activities (Ilieva & Nikolov, 2020). Additionally, IT improves daily operations by streamlining reporting and maximising the use of hardware, such as a computer, scanner, and printer, and software, such as a word processor and timesheet, or other business applications. These IT tools and technologies are beneficial for the daily operations of the organisation. At times, IT aids in corporate decision-making using digital tools and applications that facilitate idea generation and the discovery of the best solutions to challenges (Anser, et.al, 2020). Other effects of IT on business include internet-enabled systems for task coordination and data storage, which enable global expansion in this borderless IT world, as well as online recruiting of human resources (Anser, et.al, 2020).

With the significant roles of IT, the literature has emphasised the importance of regulating IT adoption within the business context via written regulations at the international and national levels, all the way down to the organisational level (Ebert, et.al, 2020; Shokouhyar, et.al, 2020). This would help ensure the business's sustainability for many years to come. Strict adherence to IT governance would thus ensure that the business model is sustainable and generates additional benefits for the company, its customers, the environment, and society.

However, issues arise regarding IT governance and its actual impact on the business's sustainable risk management policies. IT risks are continuously evolved and effected business entity in parallel with the changes in business environment. Correctly identify and manage IT risks can help organization to successfully develop and implement IT governance and control processes including methodology that enables the achievement of desired business objectives and strategies. This is especially true considering the rapid advancement of the IT and technological environments, as well as their junction with existing regulations and policies, which may be left behind considering the rapid speed of new advancements in the IT world. The best way to survive or sustain in business is through knowing and effectively managing your business risks, including IT risks. While businesses engage in IT adoption for its business and day-to-day operations, risks would inherently entail such IT adoption. Therefore, IT adoption needs to be governed in terms of its usage, handling, application, and other aspects as well. As for the risks affecting such IT adoption by the businesses, a sound risks management strategy needs to be in place to cater for the various risks. The ultimate aim of the strategy is to achieve sustainability in the business operations of the organisation particularly, and the entire business stakeholders generally. The inter-connectedness between the four domains of IT adoption, risks entailing IT adoption, IT governance and sustainability risks management (SRM) is as described in **Figure 1** below.



**Figure 1: IT Governance and Sustainable Risks Management (SRM)**

Henceforth, this study aims to examine the functions of IT governance and its effects on the practise of sustainable risk management (SRM) in Malaysia. The following sections provide an overview of the study's core concepts: IT governance, SDG9/IT sustainability, and risk management are discussed, followed by the five key functions of IT governance that have an impact on Malaysia's SRM practises.

### **Methodology**

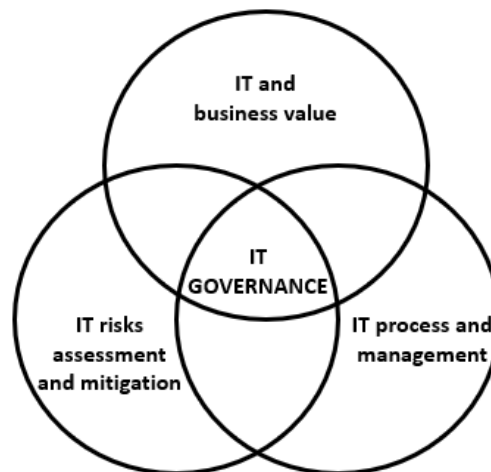
This study acquired a qualitative research method, which framed the research around documents, observations and experiences. A reach and wide range of documentary resources such as reports, policy paper, websites, news, articles and other text documents were read, skimmed, reviewed, analysed, assessed and used to perform an in-depth analysis to help draw conclusions about SRM and IT governance. The article reviews include reviewing previous literatures on IT governance and SRM. The textual data from UN Sustainable Goal Development source; especially SDG 9 is also emphasised by the researchers. Further, the researchers' experience and observations are also taken into account. Content analysis were carried out to the written materials and the results were categorised thematically. However, this paper only includes few most apparent themes resulted from the data analysed.

### **Literature Review**

This section provides an overview of the literature on the study's central themes, which are IT governance, SDG9/IT sustainability, and SRM.

#### ***IT Governance***

IT governance refers to the processes that safeguard an organisation's effective and efficient use of information technology to accomplish its goals (Larsen, et.al, 2006). IT governance has three primary objectives: I to ensure that information and technology generate business value; (ii) to monitor the performance of IT managers; and (iii) to assess and mitigate risks associated with the IT department (Gregory, et.al, 2018; Delone, et.al, 2018). **Figure 2** illustrates a generic IT governance framework. The framework is highly adaptable to the needs and operations of the organisation.



**Figure 2: Generic IT Governance Framework**

### ***SDG (Sustainable Development Goals) 9/IT and sustainability***

International and national fraternities have been pleading with IT for sustainability to regulate its adoption within business organisations. For example, the United Nations' sustainable development goals (SDGs) include 17 targets for achieving sustainability, one of which is SDG9, which is related to the study's context, namely building resilient infrastructure, promoting sustainable industrialisation, and fostering innovation. One of SDG9's objectives is to promote responsible information technology use and to call for global industrialisation and business sustainability (Sousa et al., 2018). Similarly, businesses would need to establish their own IT governance rules and policies to ensure their business, environmental, social, and governance sustainability (Anthony, 2018).

### ***Sustainability Risk Management (SRM)***

It is critical that when developing an IT governance framework for their respective organisations, they place a premium on risk assessment and mitigation, intending to achieve sustainability (Wijethilake & Lama, 2019). The term 'sustainability risk management' refers to this exercise (SRM). To put it simply, risk management is the process of embedding and integrating risk management strategies into the business organisation's IT adoption and management processes to achieve strategic, operational, financial, compliance, ethical, environmental, and social sustainability (Manab & Aziz, 2019). The SRM process is divided into five stages: (i) establish context; (ii) risk assessment of the IT adoption, implementation, and processes; (iii) risk communication; (iv) risk responses (accept, avoid, mitigation or reduction and transfer); and (v) risk monitoring and oversight. Business organisations are expected to achieve both short-term and long-term sustainability by implementing a sound SRM.

The first step in risk management is where business entities are supposed to establish the context. It formulates its objectives and strategies, develop processes, peoples, systems, structures, developing the risk criteria against which to evaluate risks and defining its internal and external environment, values and culture in which it will pursue to achieve its objectives as well as the needs and expectations of stakeholders. Specifically, in IT context, business entities need to identify the purpose and scope of the IT risk management activity and process.

Risk assessment begins with the identification of potential opportunities (positive risk) and threats (negative risks) to an organization's capacity to conduct business. These analyses aid in detecting, evaluating, and prioritizing underlying business risks, which is useful in providing mitigation methods, processes, and controls to lessen their influence on corporate operations (Cedano & Hernández-Granados, 2021). Risk assessments are undertaken in a variety of ways, depending on the risks unique to the type of business, the sector in which the business works, and the compliance laws that apply to that business or industry. The goal of the risk assessment process is to examine both threat and opportunities to establish the inherent and residual risk caused by such events (Shortland & Forest, 2020). Risks is measured in term of likelihood and impact. It means not only should dangers and their potential consequences be identified, but also strategic alliance or potential control actions to prevent any adverse effects on the organization's business operations or assets.

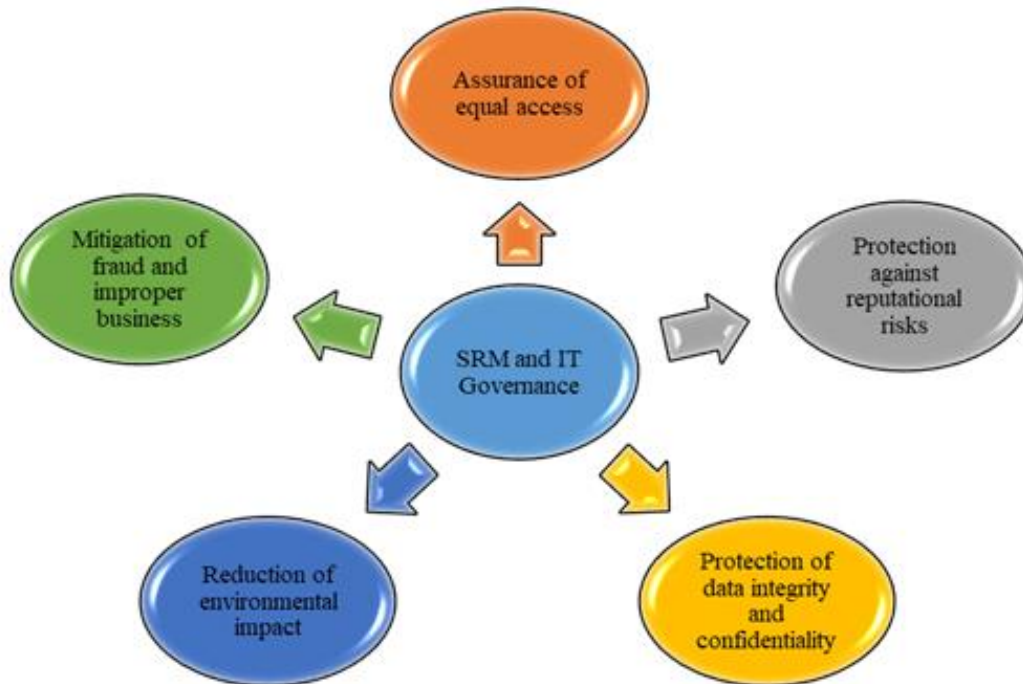
Thirdly, business entities need to understand the role of communication at various stages of the risk management process and plan, particularly in IT processes and environment. This step is critical for developing a communication strategy that is applicable to both internal and external stakeholders. Effective IT communication plan is crucial to create and execute appropriate methods, format, and contents to communicate risks with the board of directors, external stakeholders, senior management, first line, second line and third line of defenses.

The fourth stage involve risk response or treatment activity. This is where the business entities can be devise and evaluate four treatment options either to accept avoid, share, or mitigate the risks to take advantage of opportunities presented by risks consistent with entities' risk appetite. Mitigating or reducing risks means entities decide to manage the risks by making existing risk controls more reliable, devising risk treatment, implementing IT risk plans, and assessing new risks arising because of the risk treatment. It is the process of reducing an entities' exposure to potential risks in term of the impact and likelihood of those risks occurring against risk appetite, so that the risk will be reduced from unacceptable to acceptable level. Therefore, it is not sufficient for an organisation to assess and analyse diverse types of risk; it must also take action to mitigate those risks (Valerdi & Kohl, 2004). IT risk mitigation entails the application of security policies and procedures with the goal of minimising the overall risk or impact of a cybersecurity threat. Risk mitigation in information security can be divided into three components: prevention, detection, and remediation (Samimi, 2020). As cybercriminals' techniques become more sophisticated, an organisation's IT risk mitigation strategies will need to evolve to maintain an advantage.

The fifth stage of risk management is where business entities performing the risk monitoring and review roles to identify the effectiveness, quality, and appropriate aspects of each stage of the risk management process (the first four processes). Hence, monitoring allows business to warrant and devise the best practices and appropriate methods for managing risks, including deciding on appropriate risks framework and methods to report and use the information obtained. In addition, by integrating risk oversight (monitoring and review processes) into the entities' assurance agenda, entities can ensure that they are keep updated with the current changes in the business environment and to permit them to be innovative, creative and proactive to introduce continuous improvement to remain relevant, sustainable, and successful.

### Sustainability Risk Management and IT Governance in Malaysia

The study identified five critical aspects for information technology governance in promoting SRM practises in Malaysia, including ensuring equal access, protection against reputational risks, protecting data integrity and confidentiality, reducing environmental impact, and mitigating fraud and improper business, as produced in **Figure 3**.



**Figure 3: Aspects of SRM and IT Governance**

The following sections discuss each of the said aspects.

#### *Assurance of Equal Access*

One of the SDG9 goals is to ensure that all citizens, particularly those in developing countries like Malaysia, have equal and affordable access to information and communication technology. Malaysian authorities, in collaboration with technology and communication service providers, have offered a variety of incentives to ensure that citizens, particularly those living in rural areas, can benefit from technology. Regardless of the initiatives taken, if they are not closely monitored and governed, there is a risk that some citizens will be left behind. The risk of unequally shared information and technology has a significant impact on citizens, even more so in the current digital era. For example, during the Covid-19 pandemic, where vaccination information is distributed digitally via MySejahtera apps, a lack of adequate technology, such as infrastructure and Internet, resulted in vaccine distribution disparities (Press, Huisingh-Scheetz & Arora, 2021).

Additionally, Covid-19 makes online learning a requirement, rather than an option, as it was previously. The existence of technological inequality among citizens has had a profound effect on students, teachers, and parents. Inequality in access to technology and infrastructure has resulted in students having an unequal chance and opportunity to experience their formal education online. As a result, the government and service providers must work together to

ensure that the service is not only available throughout the country, but also affordable to citizens. Additionally, Williamson, Eynon, and Potter (2020) emphasised that it is not just about access, but also about the quality of access.

### ***Protection against Reputational Risks***

Numerous factors contribute to an organisation's reputation. Within the context of the Sustainable Development Goals for information technology, innovation, and infrastructure, key risks include hardware and software failure, data integrity and fake news, infrastructure and service quality, natural disasters, safety and security, privacy and confidentiality, human error, spam, viruses, cyber and malicious attacks, cyber bullying, and emotional appeal, as well as social and environmental responsibility. Failure or ineffective management of these risks will have a negative impact on the organisation's reputation. While developing a reputation can take years, sullyng it with one insecure service is trivial.

As a result, it is critical for organisations to avoid inequality and promote fair, transparent, and responsible business practises to earn the trust of stakeholders. If organisations ignore service quality issues such as internet coverage, speed, and facility gaps between urban and rural areas, they expose themselves to reputational risk. As a result, they practise inequality and have little interest in eradicating poverty in rural areas. Customers are more aware than ever of the potential reputational risks associated with their right to receive the just and equitable treatment they deserve. Additionally, they are more cognizant of the infrastructure, service quality, and protection that organisations and authorities owe them. While examining sustainability risks in business, such as ethical, social, environmental, health and safety, reputational, and moral issues, stakeholder perceptions have become more critical to organisations as they have gained increased attention in recent years. As a result, effective sustainability risk management is critical in addressing these issues and safeguarding the organisation's reputation. It is a proactive, continuous, innovative, and systematic approach to achieving organisational goals and communicating with stakeholders. As a result, the organisation's reputation must be safeguarded at all costs. A dull reputation can cause organisational disruption, while a lustrous reputation can result in organisational success.

### ***Protection of Data Integrity and Confidentiality***

Technology enables the collection of massive amounts of data, referred to as big data. As Zhang (2018) points out, while big data provides convenience for people, it also poses certain risks. As with information, our data is easily accessible to others. Occasionally, our data is shared without our knowledge. Numerous organisations store client data digitally, but these records are susceptible to being traded, shared, or stolen (Sivathanu, et.al, 2015). Data leakage can occur at any point in the data collection, storage, use, and destruction processes. If the data falls into the wrong hands, the clients will suffer (Shan, et.al, 2021). For instance, we have recently heard numerous reports of frauds. Individuals are constantly receiving calls from unknown individuals and fictitious organisations, informing us of all the fabricated stories and impending dangers. If an organisation is unable to manage their data, particularly their clients' data, they will eventually lose trust, sullyng their reputation, as mentioned previously. Thus, data governance is critical to ensuring that data is secure, accurate, and appropriately used. As a result, it is self-evident that IT governance is founded on the principle of data integrity and confidentiality (Winter & Davidson, 2019). Only through responsible IT governance can the integrity of the data be maintained, as well as the confidentiality of any data that is required to be confidential.

### ***Reduction of Environmental Impact***

The widespread use of information technology has resulted in an explosion in the number and variety of devices, particularly telecommunications devices. With the advancement of technology and the shift in people's lifestyles toward the digital world, e-waste has become one of the most rapidly growing waste streams impacting the planet, both in terms of volume and impact (Kumar, Holuszko & Espinosa, 2017). E-waste is a term that refers to electronic devices and equipment that are no longer in use or have reached the end of their useful life. Increased e-waste poses a significant risk to society and community, not just for the current generation, but also for future generations. How can this planet be sustained for future generations if it is inundated with e-waste containing hazardous toxic substances?

Additionally, the lack of consumer awareness regarding proper and efficient e-waste disposal has resulted in a significant amount of e-waste being disposed of in landfills alongside other waste (Patil & Ramakrishna, 2020). The management of e-waste generated using information technology is everyone's responsibility. According to Afroz, Muhibbullah, Farhana, and Morshed (2020), household intention to recycle mobile phones is positively related to awareness, knowledge, attitude, and costs of disposal infrastructure. Thus, the government can play a role in terms of policy and regulation, as well as educating the public about the proper way to dispose of e-waste. The Malaysian Communications and Multimedia Commission (MCMC), in collaboration with other communication companies, has initiated and implemented programmes to promote e-waste recycling. As a corporate entity, businesses can contribute in two ways: first, by reducing and reporting e-waste; and second, by ensuring that their electronic devices are easily disposed of, recyclable, and MCMC-approved.

### ***Mitigation of Fraud and Improper Business***

IT can be used either for a good or immoral purpose. In current development, it was reported that the online scam in Malaysia has been increasing from year to year and has caused losses of million dollars. Statistic shows that the number of online fraud cases recorded in 2019 was 2,512 cases involving a loss of RM28 million. This figure has increased to 5,846 cases in 2020 with a loss of RM41 million. Cases for the period from January to October 2021 plummeted to 8,997 cases involving a loss of RM58 million (Faris, 2021). The real number of cases however, could be much higher, because not all victims reported their cases to the authorities. This trend is upsetting and frightening. Government must do something to make sure that this situation can be mitigated. The introduction of the #TakNakScam campaign and the "Check Mule" application to check sellers' account information before making transaction are brilliant initial steps taken by Malaysian government towards governing the issues.

Other than government, the online business platform service providers such as Shopee and Lazada should take initiatives to ensure that the businesses register with them are legally operated and genuinely exist. Those that have registration certificate such as SSM has to be priority and entitle for exclusive offers and rewards. Beside reducing fraud possibilities, this initiative would also benefit government in increasing the number of registered online business. According to Ministry of Entrepreneur Development and Cooperatives (MEDAC), in the year 2020, there are almost two million micros, small and informal businesses that are still unregistered nationwide (Bernama, 2020). Beside ensuring business entity's existence, the service providers also need to act on customers' reports especially on the authenticity of the products sold. A mechanism needs to be introduced, to prevent the same scammers to register



to this platform using multiple accounts and defraud many different clients using different channels and names.

Besides the online business fraud, another concern is the free and world widely advertised improper and immoral business services such as prostitution or X-rated services; and shaman (especially for evil purpose). These businesses were operated unexposed traditionally, but now it become open and 'legally' advertised online and can be accessed by anyone; intentional or unintentionally. There are risks that the viewers who are unintentionally directed to these advertisements; at the end, be influenced by these services. This situation needs to be governed for the social health of our society, especially the young generations.

## Conclusion

This article examines the intersection between SRM and IT governance in Malaysia. While IT tools and applications are increasingly being used in many business organisations, it is critical that their use be governed by certain rules or standards to ensure the responsible use and management of the organisation's IT. It is a truism that, as a double-edged sword, such IT tools and applications may provide numerous benefits and advantages, such as increased productivity, improved customer relations, and others. However, such tools and applications may also present numerous threats, such as reputational risks, access inequality, environmental impact, and breach of data integrity and confidentiality.

As a result, IT governance regarding the use and management of information technology, as well as risk assessment and mitigation within the business organisation, must be aligned with SRM. This is particularly true because an effective IT governance model contributes significantly to five key dimensions of an organisation, namely assurance of equal access, protection against reputational risks, protection of data integrity and confidentiality, reduction of environmental impact and mitigation of fraud and improper business. These IT governance aspects have been found to significantly contribute to the environment's and society's sustainability, in line with SDG9's call for innovative and sustainable use of technology in daily life. The study's findings have the potential to educate business organisations about the critical nature of responsible IT governance in relation to the SRM of the business and to assist in formulating viable and appropriate rules as part of the IT governance. Thus, it is hoped that this article will serve as a catalyst and reference for future research on IT governance, sustainability, and SRM.

## References

- Abd-Mutalib, H., Muhammad Jamil, C. Z., Mohamed, R., Shafai, N. A., & Nor-Ahmad, S. N. H. J. N. (2021). Firm and Board Characteristics, and E-Waste Disclosure: A Study in the Era of Digitalisation. *Sustainability*, 13(18), 10417.
- Afroz, R., Muhibbullah, M., Farhana, P., & Morshed, M. N. (2020). Analyzing the intention of the households to drop off mobile phones to the collection boxes: empirical study in Malaysia. *Ecofeminism and Climate Change*.
- Anser, M. K., Yousaf, Z., Usman, M., & Yousaf, S. (2020). Towards strategic business performance of the hospitality sector: Nexus of ICT, E-marketing and organizational readiness. *Sustainability*, 12(4), 1346.
- Anthony Jr, B. (2018). Using green IT governance as a catalyst to improve sustainable practices adoption: a contingency theory perspective. *International Journal of Business Continuity and Risk Management*, 8(2), 124-157.

- Bernama (2020, December 12). Dua juta perniagaan kecil, informal tidak berdaftar di seluruh negara. *Sinar Harian*.  
<https://www.sinarharian.com.my/article/114479/BERITA/Nasional/Dua-juta-perniagaan-kecil-informal-tidak-berdaftar-di-seluruh-negara>.
- Cedano, K. G., & Hernández-Granados, A. (2021). Defining strategies to improve success of technology transfer efforts: An integrated tool for risk assessment. *Technology in Society*, 64, 101517.
- DeLone, W., Migliorati, D., & Vaia, G. (2018). Digital IT governance. In *CIOs and the Digital Transformation* (pp. 205-230). Springer, Cham.
- Ebert, C., Vizcaino, A., & Manjavacas, A. (2020). IT Governance. *IEEE Software*, 37(6), 13-20.
- Faris, F. (2021, November 8). Jumlah kerugian jenayah 'scam' meningkat. *Berita Harian Online*.  
<https://www.bharian.com.my/berita/nasional/2021/11/885047/jumlah-kerugian-jenayah-scam-meningkat>.
- Gregory, R. W., Kaganer, E., Henfridsson, O., & Ruch, T. J. (2018). IT Consumerization and the Transformation of IT Governance. *Mis Quarterly*, 42(4), 1225-1253.
- Ilieva, R. Y., & Nikolov, Y. P. (2020, July). IT Service Management Framework to Improve Business Information Structures. In *2020 XI National Conference with International Participation (ELECTRONICA)* (pp. 1-5). IEEE.
- Kumar, A., Holuszko, M., & Espinosa, D. C. R. (2017). E-waste: An overview on generation, collection, legislation and recycling practices. *Resources, Conservation and Recycling*, 22, 32-42.
- Larsen, M. H., Pedersen, M. K., & Andersen, K. V. (2006, January). IT governance: reviewing 17 IT governance tools and analysing the case of Novozymes A/S. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (Vol. 8, pp. 195c-195c). IEEE.
- Manab, N., & Aziz, N. (2019). Integrating knowledge management in sustainability risk management practices for company survival. *Management Science Letters*, 9(4), 585-594.
- Samimi, A. (2020). Risk Management in Information Technology. *Progress in Chemical and Biochemical Research*, 3(2), 130-134.
- Shan, L., Zhou, H., Hong, D., Dong, Q., Wang, Y., & Song, S. (2021). Application of access control model for confidential data. *Procedia Computer Science*, 192, 3865-3874.
- Shokouhyar, S., Zarrin, S., & Shokoohyar, S. (2020). Analysing the impact of IT governance on the performance of project-based organisations. *International Journal of Business and Systems Research*, 14(4), 411-433.
- Shortland, N., & Forest, J. J. (2020). Tracking terrorism: the role of technology in risk assessment and monitoring of terrorist offenders. In *Science Informed Policing* (pp. 57-76). Springer, Cham.
- Sivathanu, G., Wright, C. P., & Zadok, E. (2005, November). Ensuring data integrity in storage: Techniques and applications. In *Proceedings of the 2005 ACM workshop on Storage security and survivability* (pp. 26-36).
- Sousa, M. J., Mercadé Melé, P., & Molina Gómez, J. (2020). Technology, governance, and a sustainability model for small and medium-sized towns in Europe. *Sustainability*, 12(3), 884.
- Valerdi, R., & Kohl, R. J. (2004, March). An approach to technology risk management. In *Engineering Systems Division Symposium* (Vol. 3, pp. 29-31).

- Wijethilake, C., & Lama, T. (2019). Sustainability core values and sustainability risk management: Moderating effects of top management commitment and stakeholder pressure. *Business Strategy and the Environment*, 28(1), 143-154.
- Winter, J. S., & Davidson, E. (2019). Big data governance of personal health information and challenges to contextual integrity. *The Information Society*, 35(1), 36-51.