Manuscript Submitted	28.5.2024
Accepted	10.6.2024
Published	30.6.2024

Information Security Risk Assessment Measures of Facility Management in Transport Industry

Abdul Halid Ramli, Nurazean Maarop, Muhammad Syahreen Zulkifli, Ganthan Narayana Samy, Noor Hafizah Hassan, Roslina Mohammad

Faculty of Artificial Intelligence
Universiti Teknologi Malaysia

halid@tbsbts.com.my, nurazean.kl@utm.my, muhammadsyahreen@graduate.utm.my, ganthan.kl@utm.my, noorhafizah.kl@utm.my, mroslina.kl@utm.my

DOI: https://doi.org/10.53840/myjict9-1-142

Abstract

The objective of this study is to identify the necessary information security measures for facility management (FM) firms in the transportation industry to control risks. This study was founded on the three phases of the OCTAVE framework, the Information Security Risk Assessment checklist, the nine stages of NIST SP800-30 2012, and ISO 27005:2011 on Information System Risk Management. This study finalized eight significant risk management measures for FM enterprises based on a descriptive analysis of sixty questionnaires containing responses from key respondents employed by FM companies in Malaysia. Beforehand, the information security experts reviewed and validated the appropriateness of the following measures for managing risks in this study context: system characteristics; threat identification; vulnerability identification; control analysis; likelihood determination; impact analysis; risk determination; and recommendation for controls. Consequently, the result of this study reveals the outcomes of descriptive analysis comprising mean and standard deviation for the information system security measures for risk management of the respective transport company. Lastly, our research could be advantageous to FM companies, particularly those in the transportation industry, by providing standardized measures for managing information security risk.

***Keywords*:** *Information Security Risk Assessment, Risk Assessment Measures, Information Security, Facility Management*

1. Introduction

Facilities Management (FM) is an industry that provides maintenance, user management, and project management support (Cigolini et al., 2009). In the past two decades, the FM market has expanded dramatically. Increasing government spending on transportation, building, operations, and upkeep contributed to the growth. For example, the government of Saudi Arabia estimates that the Facilities Management Industry will produce USD 36 billion for transportation projects. Global revenue from facilities management is expected to reach $1,759.25 billion during the coming decade (Fortune, 2022).

The facility management industry's developments are determined by technological advancements and company strategies. In addition to the advantages of information technology, the rising complexity of technology presents numerous security risks for FMs (Nota et al., 2021). Owing to technology innovation acceptance in operations, the FM sector currently offers a variety of solutions, services, processes, and policies to safeguard the confidentiality, integrity, and availability of ICT-supported business functions within an organisation (Marcinkowski & Gawin, 2020).

In the new industrial revolution 4.0, the majority of businesses, including FM, initiated formal information security management plans within their organisations. Implementing rules and regulations, or a system that combines people, procedures, and technology, is intended to secure the organization's overall assets (Choubey & Bhargava, 2018). This approach supports the organization's viability and growth (Fenz et al., 2014). The accepted reference benchmarks and comparative methodology for evaluating this ISRA approach for assessing information security risks are, however, lacking. Before selecting the suitable ISRA approach to complete the risk assessment, organisations would often do a thorough comparative analysis of the different methodologies (Shedden et al., 2016).

Thus, the high costs associated with adopting and maintaining security measures increase the pressure on facility managers to distinguish between controls that their businesses require and those that are less essential. The difficulty is determining what security plan firms should implement to protect their most valuable assets and people during an attack, as well as how to avoid and conduct countermeasures. It may be difficult to find the appropriate procedures for identifying, detecting, responding to, and recovering from imminent dangers. Thus, the selection of controls from the various security frameworks could determine the success or failure of implementation (Abdullah et al., 2015).

Several standards related to frameworks for information security. Various ISRA frameworks have distinct controls; some may not be suitable for companies. In addition, there are no precise criteria that a firm can adhere to unless it develops its own comprehensive information security checklist (Groš, 2021). Hence, the intent of this study is to discover the measures that facility management (FM) companies operating in the transportation sector need to undertake in order to mitigate possible risks.

2. Literature Review

Calculating the severity of an exploited vulnerability is one of the most important components of ISRA. If the severity is anticipated to be severe, somewhat stringent preventive actions should be taken. Suppose, however, that the severity is deemed insufficient. In this situation, the deployment of costly defence tools could cause the FM's organisation to incur a loss. Hence, achieving the optimal and accurate balance is essential (Shameli-Sendi et al., 2016). The following sections provide reviews of relevant standards that may be taken into account when selecting the appropriate metrics to be used in this study.

2.1 ISO27005:2011

The ISO 27001 cycle of documentation involves a periodic risk assessment when new features and products are added. The processes include risk assessment and management, control selection, internal audit, monitoring, and certification, which followed the PDCA cycle (Agrawal, 2017). Yet, industry best practises may be extremely expensive, deliver insufficient data, and impede the administration and delivery of services (Weil, 2020). In Fig. 1, the ISO/IEC 27005:2011 ISRM procedure is shown. As depicted in the graphic, risk assessment is an integral component of ISRM, which encompasses a broad range of issues.

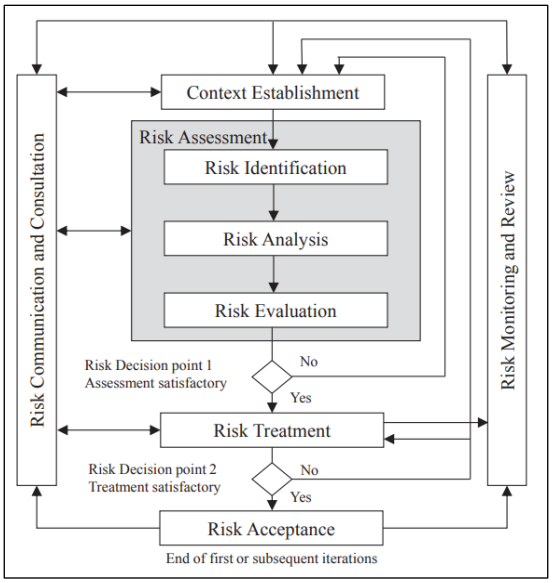

Figure 1: ISO/IEC 27005:2011 ISRM process (Wangen et al., 2018)

2.2 OCTAVE

The OCTAVE is an operationally critical threat, asset, and vulnerability assessment. Initially, OCTAVE consists of three phases. The three phases are as follows (Suroso and Fakhrozi, 2018): building asset-based threat profiles, identifying infrastructure vulnerabilities and developing a security strategy and plans. Despite the nonlinear nature of the approach, phase 3 is dependent on phases 1 and 2. OCTAVE has been refined and improved over a number of versions. OCTAVE Allegro, which is the version on which this part concentrates, is designed to be a lightweight and less burdensome method to deploy (Caralli et al., 2007).

2.3 NIST SP800-30, 2012

The National Institute of Standards and Technology's ISRM standard is another well-known ISRM standard (NIST). NIST SP800-30 as shown in Fig.2 is a guide for conducting risk assessments for security. It provides instructions for conducting the tasks of a risk assessment process, which include preparing for, conducting, communicating the results of, and maintaining the assessment. The NIST SP800-30 framework divides activities into six stages. Identifying assets and vulnerabilities are the first two steps. Other stages include determining the effectiveness of security controls and assessing the negative impact of risks as a combination of impact and likelihood. Similar to the ISO 27005 standard, the first phase concentrates on ISRA preparation. NIST SP800-30 is a flexible framework that offers a standard report structure and is utilised by numerous organisations in the United States, most notably the aerospace industry (Pereira et al., 2017).

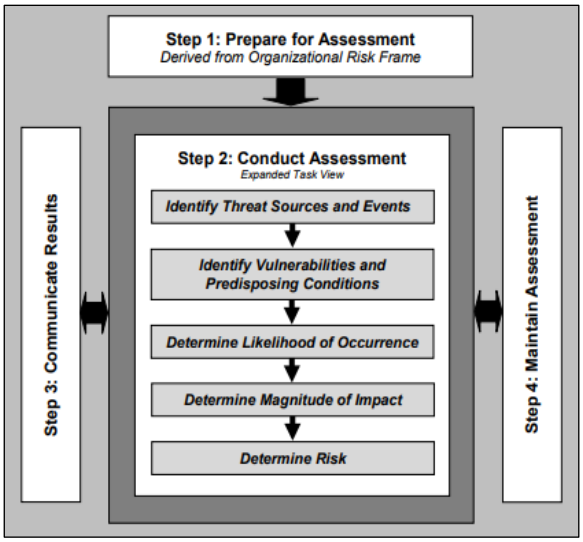

Figure 2: Risk Assessment Process (NIST, 2012)

2.3 Element in Risk Management Framework

Based on the three distinct ISRA frameworks, this project identifies the control measures suitable for the FM's operational risk assessment. The following Table I. shows the elements of the three frameworks connected to risk management measurements, hence displaying the common ground between the three.

Table 1: Measures of Three Main ISRA Frameworks

NIST SP 800-30 Risk Assessment (NIST, 2012)	**ISO 27005 Information Security Risk Management** (Wangen et al., 2018)	**OCTAVE Allegro** (Caralli et al., 2007)
Prepare Assessment, System Characterization	Context Establishment	Establish Risk Measurement Criteria
Threat Identification	Risk Assessment	Develop Information Asset Profile
Vulnerability Identification	Risk Analysis – Risk Identification	Identify Information Asset Containers
Control Analysis	Risk Analysis – Risk Estimation	Identify Areas of Concern
Likelihood Determination	Risk Evaluation	Identify Threat Scenarios
Impact Analysis	Risk Treatment	Identify Risk
Risk Determination	Risk Acceptance or	Analyze Risk
Communicate Result and Maintain Assessment	Communication, and Redo, Risk Monitoring and Review	Select Mitigation Approach

This study's subsequent work was founded on these commonly used metrics that were surveyed among FM industry professionals.

2.4 Selected Measures in ISRA For FM

Based on the three distinct ISRA frameworks, this project selects the following:

- System Characteristic: The characteristics of the system include asset management for servers, workstations, storage and backup, network apparatus, network segments, applications, data

repositories, virtual technologies, and service providers. Despite the absence of an asset-based risk assessment, configurations of datacentre systems were maintained and enhanced annually (Weil, 2020). According to (Suroso and Fakhrozi, 2018), asset management may also be broken down into these three categories namely Technical (Hardware, software, or a system internal and external to the organisation), Physical (The physical location or document controlled by the business (internal) but not by the industry (external)), and Individuals (those with access to both organization-controlled (internal) and non-organization-controlled (external) information about FM).

- Threat Identification: In the industry, technology and business management are evolving swiftly. With competition from new players in the market and liberalization, the quality of products and services has significantly increased. The identification of risks remains the foundation of a systemic risk assessment for industrial activity. The objective is to gain a thorough comprehension of the relevant issues. Then, it may provide FM organizations with the confidence to make risk-informed decisions for risk protection (Zio, 2016). Four activities may be considered to identify the threat to the organization's assets (Wangen et al., 2018) and these are on-site interviews, questionnaires, physical inspection and document review.
- Vulnerability Identification: Vulnerability and risk assessments safeguard systems. The system's objectives, cascade effects on the recognized design, and acceptable event sequences must be addressed for calculating resilience (Aven, 2016). Unknown hazards cannot be handled; hence dangers must be assessed without leaking. Vulnerability as a system attribute adds three features (Zio, 2016) which are risk-related losses and damages, risk exposure and resilience.
- Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersted. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
- Control Analysis: A threat, according to ISO27005, is a sort of damage or loss. On the other hand, OCTAVE Allegro specifies that the danger is either a human or a technical issue. At the same time, according to ISO27005, this is a cause of risk for the organization. Threats are addressed in the NIST 800-30 risk assessment method, which markets itself as a threat-based risk assessment approach. However, it only includes two of the four recognized threat assessment categories during the risk estimation phase (Wangen et al., 2018).
- Likelihood determination: The ISO 31000 risk management standard defines probability as “the chance of something happening.” Information Security Risk Management ISO 27005 uses this definition. The NIST Special Publication 800-30 Guide for Conducting Risk Assessments defines likelihood of occurrence as “the probability that a given threat is capable of exploiting a given vulnerability or set of vulnerabilities.” ISO27005 defines threats as harm or loss. Risk estimates produce OCTAVE Allegro's risk score (Wangen et al., 2018).
- Impact Analysis: Few studies on impact analysis provide guidance on how to select measures for identified risks. Impact analysis offers techniques for modelling the relationship between assets, hazards, and mitigation measures and determining logically the most effective combinations of mitigation measures. The selection of measurements can be formulated as discrete optimization problems (Kawasaki & Hiromatsu, 2014).
- Risk Determination: Risk management requires risk acceptance (Elena & Johnson, 2015). Thus, risk acceptance refers to how many organizations accept hazards from using the cloud computing platform. Risk management requires risk acceptance. Risk acceptance criteria improve IS and provide the company with a competitive edge. Most FM organizations use broad internal risk categorizations instead of standards to determine an acceptable risk level for external suppliers (Kumar et al., 2018).
- Control Recommendation: Risk-related control recommendations are assessed financially. Decision-makers can reduce risks by categorizing them in order. ISRA professionals must analyses important asset linkages, threats, and weaknesses. ISRA practitioners usually highlight critical asset security and risks (Shamala et al., 2013). ISRA emphasizes that most risk

management methods do not involve training, meetings, workshops, risk updates, monitoring, or reassessment.

3. Methodology

This project employed a quantitative methodology for data collection and analysis was done descriptively. It entails gathering information from selected Information technology and information security professionals from FM's operational organizations that administer transport terminals. Beforehand reviews of measures items were done by three experts of information security both from industry and academic circle. The experts validated the suitability of the following measures for risk management: system characteristics; threat identification; vulnerability identification; control analysis; likelihood determination; impact analysis; risk determination; and recommendation for controls. After taking expert feedback into account, the final version of the measures is sent to the FM company involved. We used the importance-scale question as it is a form of question employed in numerous surveys. These five-point rating systems range from 1 (not important) to 5 (extremely important). This question seeks to evaluate the relative importance of various decision-making factors. The data was then imported into Microsoft Excel. We employed frequency, mean and standard deviation analysis to demonstrate the response trend of the participants.

4. Analysis and Result

The survey evaluates the proposed measures of Information System Security Risk Assessment from the perspective of Transportation Facility Management company utilizing the facilitating measures laid out in this research. This survey collected sixty responses from the Facility Management company to measure the information systems security risk checklist in the company and analyse the responses based on descriptive statistical frequency.

4.1 Demographics

The demographic information includes gender, age, position within the organisation, number of IT professionals, and years of experience and these are shown in Table 2.

Table 2: Demographics

Category		**Frequency**	**Percentage**
Gender	Male	28	46.7
	Female	32	53.3
Age	21-29	11	18.3
	30-39	42	70
	40-49	4	6.7
	50-59	1	1.7
Category		**Frequency**	**Percentage**
Position Category	Information Technology Officer	40	67
	Management Team	20	33.3
Work Experience	Less than 5 years	15	25
	5- 10 years	15	25
	11-20	12	25
	More than 20 years	18	30

4.2 Information Security Risk Assessment Measures

Based on the literature review and experts' recommendation, this study finalized the following measures. System Characteristics (SC): The requirement for asset management for servers, workstations, storage and backup, network equipment, network segments, applications, data repositories, virtual technologies, and service providers. The threat identification (TI) process examines IT vulnerabilities and determines their capacity to compromise your system. It's a key element of your organization's risk management program. Identifying threats allows your organization to take pre-emptive actions. The vulnerability identification (VI) process enables the organization to identify and understand weaknesses in the system, underlying infrastructure, support systems, and major applications. Control Analysis (CA) is a key element used to derive the final Risk Determination.

Since it is an intermediary step in the process it is better suited to be presented in its own container rather than the report body itself. Likelihood determination (LD) represents the most likely consequence occurring in the event of a hazard occurrence. Impact Analysis (IA) is the key aspect of responsible requirements management by providing an accurate understanding of the implications of a proposed change, which helps the teams make informed business decisions about which proposals to approve. Risk determination (RD) assesses threats and vulnerabilities to consider the likelihood that known threat sources will be able to exploit identified vulnerabilities to cause one or more adverse events and the consequences of such events occur. Control recommendation (CR) is possible course of action for any risk identified and evaluated in the risk management process, thus risk managers need to consider potential responses to risk, alone or in combination and identify the possible courses of action. Table 3 displays the results of the analysis with mean, and standard deviation (SD) values.

Table 3: Important-Scale Analysis on Measures (N=60)

Measure	Mean	SD
SC1: Asset management pertaining to technical aspects, such as hardware, software, and systems associated assets.	4.42	0.690
SC2: Asset management for physical location such as business address and data center including disaster recovery.	4.13	0.618
SC3: Person access to both organization-controlled (internal) and non-organization controlled (external) information and locations related to FM's operations.	4.90	0.30
TI1: Threats Identification through on-site interviews including the individual screening process.	4.07	0.813
TI2: Threats Identification through questionnaire to determine the possibility of occurrence of some situations that could generate losses.	4.68	0.532
TI3: Threats Identification through inspection, visit to the facilities and physical contact with the members of the inspection team with the environment.	4.67	0.674
TI4: Threats Identification through Document Review such as process flowchart, SOP, financial statement, and insurance policy	4.00	0.930
VI1: Vulnerable identification through losses and damages assessment	4.18	0.785
VI2: Vulnerable identification through risk exposure is dynamic, varying across temporal and spatial scales, and depends on economic, social, geographic, demographic, cultural, institutional, governance, and environmental factors.	4.42	0.736

VI3: Vulnerable identification through measuring the accepted resilience of an entity to resist or recover from damage	4.00	0.774
CA1: During risk analysis, the goal is to learn the nature of the risk(s).	4.38	0.776
CA2: During risk analysis, Facility Management considers uncertainties, sources of risk, likelihood of events, and measures the effectiveness of current controls.	4.25	0.849
CA3: During risk analysis, Facility Management consider uses a high-quality, accurate, and complete information.	4.47	0.694
LD1: The likelihood levels can be described as frequency values or with respect to how easy it is for a person to exploit a threat.	4.57	0.738
LD2: The likelihood of an event can be measured based on qualitative (such as reputation damage) and quantitative (such as system downtime) approaches.	4.68	0.645
LD3: The likelihood of an event can be determined based on the level of occurrences such as very high, high, moderate and low.	4.78	0.579
IA1: Traceability impact analysis captures the links between requirements, specifications, design elements, and tests, analyzing their relationships to determine the scope of an initiating change.	4.42	0.801
IA2: Dependency Impact Analysis is used to determine the depth of the impact on the system.	4.63	0.682
IA3: Experiential Impact Analysis studies what happened in similar situations in the past to determine what may happen in the future through experts in the organization.	4.83	0.453
RD1: Risk determination assesses threats and vulnerabilities to consider the likelihood that known threat sources will be able to exploit identified vulnerabilities.	4.43	0.803
RD2: Organizations characterize the nature and severity of adverse impacts according to what aspect of security is impacted, the extent of disruption to operations, the resources lost, or the consequences to mission execution or organizational stakeholders.	4.42	0.824
RD3: Accurate quantitative risk determination requires sufficient historical observations or other evidence to support calculation of probabilities, and also requires impact to be expressed in numeric terms.	4.80	0.542
CR1: Risk acceptance falls within the organizational risk tolerance, and accepting the risk may be justified.	4.70	0.641
CR2: Risk mitigation includes remedial or corrective action taken to reduce the level of risk to the organization, with the goal of bringing the risk level within organizational risk tolerance so that any residual risk can be accepted.	4.87	0.464
CR3: Risk-sharing occurs when responsibility for the risk borne by one organization can be shared with another, in a manner that may not reduce the total risk, but reduces the risk faced by each sharing organization to an acceptable level.	4.53	0.763
CR4: Risk transfer by shifting responsibility or liability for the consequences of an adverse event to another organization, such as by purchasing insurance against loss or harm.	4.82	0.499
CR5: Risk avoidance deals with eliminating any exposure to risk that poses a potential loss to the organization and can be achieved through policy and procedure, training and education, and technology implementations.	4.63	0.632

The majority of the feedback indicates that the majority of the measures are above the 4-important scale and near to the 5-extremely important scale, indicating that the majority of the measures are of high acceptability importance. In particular measures related to likelihood determination and control determination are scaled higher than all other measures.

5. Conclusion

The FM operations should be designed to protect the confidentiality, availability, and integrity of business functions supported by ICT. Hence, this study endeavors to address the existing challenges in information security risk among transportation industry facility management firms. This study also proposed ISRA measures that integrates a risk assessment procedure, including identification, estimation, and evaluation of risks. This study outlined the significance of the proposed ISRA measures through a quantitative survey of FM company's main respondents. In future, this study suggested evaluating the effectiveness of the proposed Information Security Risk Assessment measures by demonstrating their application within FM companies.

Acknowledgments

We would like to thank Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia.

References

Cigolini, R. D., Van der Zwan, J., Straub, A., Martinez, D., Aiello, G., Mazziotta, V., & Micale, R. (2009). Facility management, outsourcing and contracting overview. In Recent advances in maintenance and infrastructure management (pp. 225-290). Springer London.

Fortune Business Insight. (2022). Market Research Report. https://www.fortunebusinessinsights.com/industry-reports/facility-management-market-101658.

Nota, G., Peluso, D., & Lazo, A. T. (2021). The contribution of Industry 4.0 technologies to facility management. International Journal of Engineering Business Management, 13, 18479790211024131.

Marcinkowski, B., & Gawin, B. (2020). Data-driven business model development–insights from the facility management industry. Journal of Facilities Management, 19(2), 129-149.

Choubey, S., & Bhargava, A. (2018). Significance of ISO/IEC 27001 in the implementation of governance, risk and compliance. International Journal of Scientific Research in Network Security and Communication, 6(2), 30-33.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. Information Management & Computer Security, 22(5), 410-430.

Shedden, P., Ahmad, A., Smith, W., Tscherning, H., & Scheepers, R. (2016). Asset identification in information security risk assessment: A business practice approach. Communications of the Association for Information Systems, 39(1), 15.

Abdullah, N. A. S., Md Noor, N. L., & Mior Ibrahim, E. N. (2015). Contributing factor to business continuity management (BCM) failure-A case of Malaysia public sector.

Groš, S. (2021). A critical view on CIS controls. In 2021 16th International Conference on Telecommunications (ConTEL) (pp. 122-128). IEEE.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & security, 57, 14-30.

Agrawal, V. (2017). A framework for the information classification in ISO 27005 standard. In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 264-269). IEEE.

Weil, T. (2020). Risk assessment methods for cloud computing platforms. IT Professional, 22(1), 63-66.

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF. International Journal of Information Security, 17, 681-699.

Suroso, J. S., & Fakhrozi, M. A. (2018). Assessment of information system risk management with octave allegro at education institution. Procedia Computer Science, 135, 202-213.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing octave allegro: Improving the information security risk assessment process. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.

National Institute of Standards and Technology.: NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments (2012).

Pereira, D., Hirata, C., Pagliares, R., & Nadjm-Tehrani, S. (2017). Towards combined safety and security constraints analysis. In Computer Safety, Reliability, and Security: SAFECOMP 2017 Workshops, ASSURE, DECSoS, SASSUR, TELERISE, and TIPS, Trento, Italy, September 12, 2017, Proceedings 36 (pp. 70-80). Springer International Publishing.

Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety, 152, 137-150.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253(1), 1-13.

Kawasaki, R., & Hiromatsu, T. (2014). Proposal of a model supporting decision-making on information security risk treatment. International Journal of Economics and Management Engineering, 8(4), 583-589.

Elena, G., & Johnson, C. W. (2015). Factors influencing risk acceptance of cloud computing services in the UK government. arXiv preprint arXiv:1509.06533.

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, 691-697.

Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). Journal of Information Security and Applications, 18(1), 45-52.