Framework for Digital Data Access Control from Internal Threat in the Public Sector

Haslidah Halim[1]
ICT Consultation Unit
MAMPU, Cyberjaya, Malaysia

Maryati Mohd Yusof[2]
Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia, Bangi, Malaysia

***Abstract*—Information management is one of the main challenges in the public sector because the information is often exposed to threat risks, particularly internal ones. Information theft or misuse, which is attributed to human factors, affects the reputation of public sector organizations due to the loss of public trust in the security and confidentiality of the information and personal data that are hacked by internal parties. Most studies focus on general problem solving related to internal threats instead of digital personal data protection. Therefore, this study identifies the main security control elements for personal data access in the public sector, including information security management, human resource security, operational security, access control, and compliance. A comprehensive framework is developed based on the identified security control elements and validated using a case study. Data are collected using interview, observation, and document analysis techniques. The findings contribute to the management of information system security through a systematic approach to controlling internal threats in the public sector. This framework can serve as a guideline for the public sector in managing internal threats to reduce security incidents involving unauthorized access to digital personal data.**

***Keywords*—Information management; internal threats; control framework; risk; information security; personal data access**

I. Introduction

Information is a critical asset in organizations. Therefore, it must be secured and protected from any modification, unauthorized use, and integrity loss [1-4]. Organization information is prioritized to ensure constant security and protection to prevent leakage to unauthorized parties. Information leakage affects organization reputation due to loss of trust in securing information from external entities.

Information systems (IS) are vulnerable to various threats, which can lead to undesired and costly consequences, including breach of data confidentiality or integrity and system unavailability [5]. Threats are attributed to internal and/or external entities. Internal threats have pervasively become a critical and serious concern in most public agencies and industries [6,7]. Most internal attacks are attributed to human factors [8-10]. According to Shu et al. [11], sensitive data leakage from computerized systems has also become a serious threat to organizational security.

Previous studies focused on solutions to general internal threats instead of internal threats pertinent to personal data [12]. Personal data are defined as processed information (partial or complete) in commercial transactions that are directly or indirectly related to individual data subjects, enabling data identification from that information or other information matching based on data related to a user. Therefore, the current work identified the main elements of security control, and these elements were utilized as the foundation of the proposed framework for internal threat control in accessing digital personal data in the public sector. The framework was developed based on a critical analysis of the literature on internal threats and of previous frameworks on policy and information security management, human resource and operational security, and access and compliance control.

This paper is divided into seven sections. Section I outlines the introduction. The literature review is discussed in Section II, and information security management and frameworks on internal threats to information security are explained in Section III. The proposed framework is described in Section IV, and the methods, results, discussion, and conclusion are presented in Sections V, VI, VII and VIII, respectively.

II. Information Security Management

Information management success is an antecedent for establishing and maintaining organization competitiveness [13]. Organization information management should be aligned with the aspect of information security to ensure information validity and accuracy. IS security in the public sector is crucial due to its role as part of critical organization infrastructure, encompassing personal or sensitive data [14]. IS in the public sectors are different from that in the private sector. IS failure in the public sector can considerably disrupt various economic and social activities and harm human life (such as failure in emergency service systems). IS security is becoming increasingly challenging due to emerging Internet-based applications, including e-commerce and various information selling services. Therefore, IS must be designed with guaranteed confidentiality, integrity, availability, authenticity, and auditability [15].

The main concern among security experts is minimizing threats from internal individuals [9, 16]. Data leakage and selling are pervasive due to hidden web site use and convenience in leaking confidential data without traces or names. Moreover, most internal attacks involve skilled and knowledgeable individuals [17].

Problems or failures in information security are normally attributed to human actions and can lead to costly losses [9, 10, 18, 30]. However, Hashem et al. [19] argued that internal

We greatly appreciate funding received from the Universiti Kebangsaan Malaysia (DIP-2016-033) and Malaysian Public Service.

threats are inevitable but can be avoided in the early stages. Therefore, a comprehensive framework for monitoring and detecting internal threats is essential for early detection.

ISO/IEC 27001/27002 is an International standard that has been widely applied in information security management. The public sector also uses this standard to protect critical information and address intrusion risks, which can lead to leakage in official government information. ISO/IEC 27001/27002 provides a framework that guides organizations in implementing the International Information Security Management Standard (ISMS) [20]. ISO/IEC 27001:2013 [21] outlines requirements for establishing, implementing, maintaining, and continuously enhancing information security management in organizational contexts. The standard also features requirements for evaluating and maintaining information security risk based on organization needs. The Malaysian government has established a cyber-security framework for the public sector [22] to provide basic guidelines that include all necessary security components that must be considered by government and public agency sectors to protect information in their cyberspace. This study employed 14 security control elements from ISO/IEC 27001:2013 [21] as bases for information security due to their inclusion in the ISMS standard. A critical analysis of previous frameworks was conducted to identify elements related to data access control.

III. Internal Threat for Information Security Framework

Three frameworks related to internal threats were identified from the literature based on their relevance, suitability, and popularity in providing solutions to problems related to such threats. These frameworks are 1) adaptive risk management and access control framework [23], 2) insider threat security architecture (ITSA) [24], and 3) management policy for access control from a system user perspective in collaborative environments [13]. These previous frameworks were compared against security control elements in ISO/IEC 27001:2013 [21] (Table I).

The framework of Baracaldo and Joshi [23] emphasizes human resource, access control, and compliance for internal users. The framework also includes risk management by considering user behavior. All security control elements in application systems are critical for minimizing internal threat risk in general and information misuse in particular.

The ITSA framework [24] is nearly complete and contains most of the security control elements in ISO/IEC 27001:2013. The framework features six security control elements, namely, information security basis, information security management, human resource security, operational security, access and compliant control for handling internal threat problems. In addition, policy elements are adopted, wherein access control is aligned with organization policy compliance. The framework acts as a control mechanism to address internal threat problems that stem from authorized system users. Moreover, ITSA framework [24] used audit elements in the monitoring process by recording audit trails, reports, and analyses in integrated business intelligence components that are appropriately aligned with compliant elements that require user activity to be recorded for security purposes.

The framework of Ahmad et al. [12] combines several security control elements, namely, information security management basis, human resource security, access and compliance control for handling internal threats. Ahmad et al. [12] provide autonomy to data owners by enabling their direct involvement in managing policy for data access. All security control elements in application systems are critical for minimizing risk caused by unauthorized use or information theft by authorized users.

All three frameworks use the same security control elements, namely, information security basis, information security management, human resource security source, access and compliance control for handling internal threat problems in organizations. Only the ITSA framework [24] adopts operational security elements whereas that of Baracaldo and Joshi [23] includes risk management elements.

TABLE. I. Framework Comparison based on Security Control Elements in ISO/IEC 27001:2013

	Framework		
Security elements ISO/IEC 27001:2013	**Baracaldo and Joshi [23]**	**ITSA [24]**	**Ahmad et al. [13]**
Information security basis	Available	Available	Available
Information security management	Risk management and control access	Audit Security (threat prevention)	Application and database management
Asset management			
Human resource security	Control via monitoring, context, and trust modules	Authorization of access control	Access control on user and data owner
Physical and environmental security			
Cryptography			
Operational security		Audit trail logs Reporting and analysis	
Communication security			
Access control	Available	Available	Role-based access control
IS acquisition, development, and maintenance			
Management of security incidents			
Supplier relationship			
Service continuity management			
Compliance	Compliance Policy enforcement	Policy compliance Management order Rules and regulations	Policy implementation

The literature on internal threats was reviewed to identify additional elements for security control in handling internal threat problems. Security documents regarding government ICT and Personal Data Protection Act 2010 [25] were also analyzed considering the study scope in developing a framework for internal threats to protect digital personal data for public service use. Six security control elements and three additional elements were identified from the literature (Table II). In short, the six main security control elements, namely, information security basis, information security management (ISM), human resource security, operational security, access and compliance control, are critical in handling internal threats for accessing the digital personal data of the public sector. Security control implementation is supported by three additional elements in PDPA, namely, risk management, cryptography, and access principle. All six security control elements and the three additional elements served as the foundation for developing the proposed framework for internal threat control from personal digital data access (PDDAITC) in the public sector.

The framework by Ahmad et al. [12] was adopted and extended by adding five new elements, namely, internal threat control, security policy control, application control, database control, and security control. The comparison of the proposed framework and that of Ahmad et al. [12] is shown in Table III.

TABLE. II. SECURITY CONTROL AND ADDITIONAL ELEMENTS

	Elements	**References**
Security control elements		
1	Information security policy	[15,23,24,26,33]
2	Information security management	[14,15,23,24,26,31]
3	Human resource security control	[15-17,18,19,23,24,26-28]
4	Operational security	[23,24,26]
5	Access control	[6,23,24,26,33]
6	Compliance	[23,24,26,30,32,33]
Additional elements of security control		
1	Risk management	[3,15,22,25,31,33]
2	Cryptography	[2,11]
3	PDPA – access principle	[25,33]

TABLE. III. COMPARISON OF THE PROPOSED FRAMEWORK WITH THAT OF AHMAD ET AL. [12]

Ahmad et al. [13] Framework	**Proposed Framework (PDDAITC)**	
User Data admin/ owner	Internal threat source	User Data administrator/ owner
Server policy	*Application control	Access control (id, password, cryptography) System authorization control
Database	*Database control -data owner autonomy	Access control (id, password, cryptography) Audit trail Encryption
Policy - Data owner determines data access policy	*Security policy control	ISM ISMS standard Risk management PDPA
	*Internal threat control	Access control policy Guideline/SOP ICT security policy Operational security
	*Security control	Compliance

IV. PROPOSED FRAMEWORK

The proposed framework was developed using a holistic approach by adapting the framework of Ahmad et al. [13] and conducting a critical analysis of the literature related to internal threats and control elements (Fig. 1). Six security control elements and three additional elements are classified as security components, namely, internal threat control, security policy control, application control, database control, and security control. All proposed security elements are featured in ISO/IEC 27001:2013 [21] security elements, which are also encompassed in the reviewed frameworks [12, 23, 24]. Users and data owners, which are classified as sources of internal threats, must comply with all security controls.

Before access is granted, data owners must comply with security policy control, which comprises ISM, risk management, standard organization ISMS, and PDPA. Data owners must also adhere to database control security, which includes access control element, audit trail, and encryption. Access control authorization for data owners is only verified through user ID, password, and cryptography. Data owners are granted autonomy on their data based on the access principle in PDPA. Users and data owners must comply with all security control categories in the proposed framework to secure organization control from any undesired security incident. The following security control elements and their implementation approaches are outlined.

1) All appointed officers, staff, and suppliers must comply with the information security policy. Violation of information security can affect confidentiality, integrity, and information availability.

2) Security control of human resource is a critical element in controlling internal threats in organizations. The security filter in a non-disclosure agreement (NDA) is a document that must be signed by suppliers and recorded in a system. All officers, staff, and appointed suppliers must also sign and comply with the security policy of organization ICT.

3) Information security management is an important element that must be considered by organizations because any leakage or unauthorized use of information can affect organizational reputation. Undesired incidents are controlled and prevented through ISMS organization security policy.

4) Operational security - Application and database operation are monitored based on SOP or guidelines to ensure the smooth daily operation and avoid undesired security incidents.

5) Application and database access control is determined in accordance with the role, job scope and work duration of officers, staff, and suppliers. Access cancellation for relocated, retired, or terminated staff must be immediately activated to minimize risks of security threat toward the organization.

6) Compliance - Security or guideline policy and SOP must be fulfilled to ensure enforcement on appointed officers, staff, or suppliers. Follow-up action must be executed against security incidents pertinent to security information.

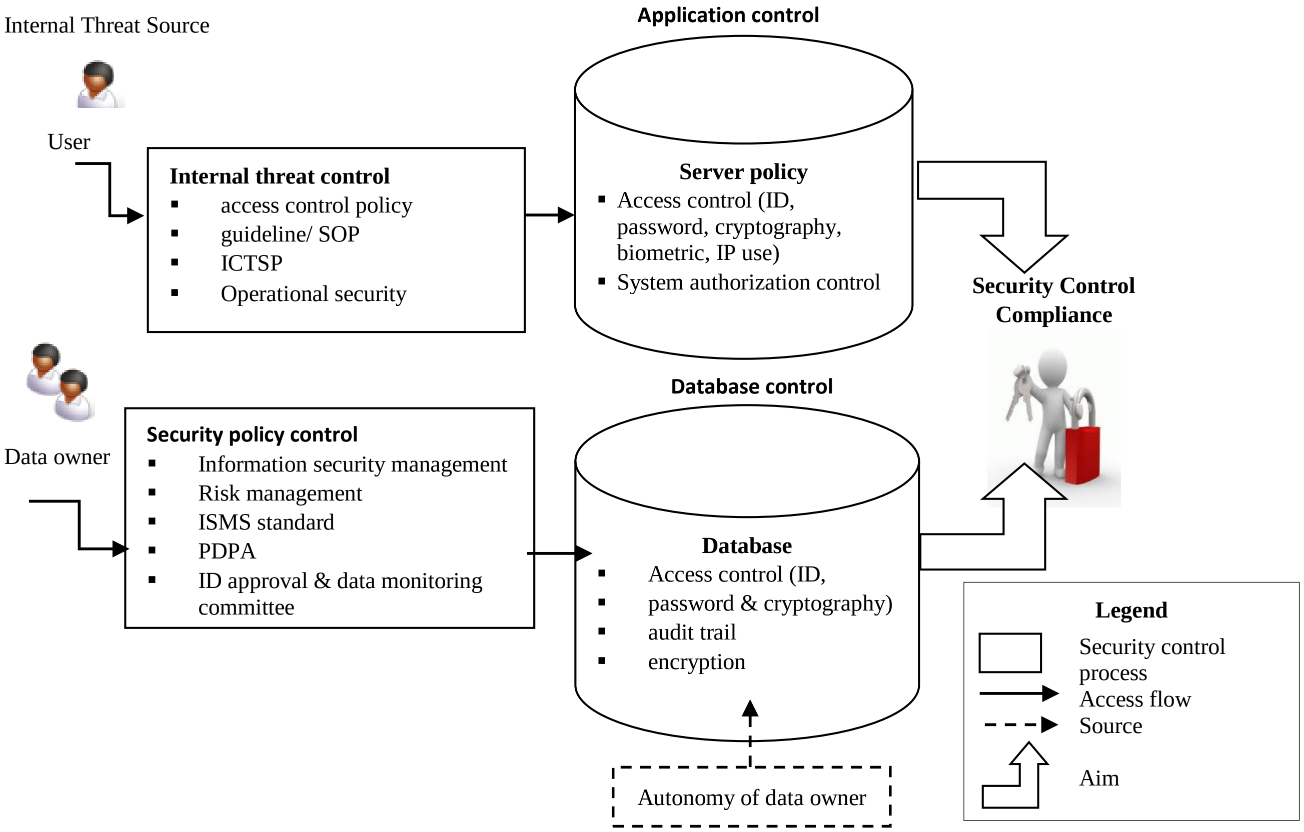

Fig. 1. Framework for Internal Threat Control for Digital Access Control in Public Sector.

The following are additional elements that support the implementation of security control:

1) Risk management is identified and monitored through the enforcement of information security policy on appointed officers, staff, or suppliers to reduce intentional or unintentional threat risk.

2) Cryptography is implemented on applications and databases to increase the security of information stored in the organization.

3) Access principle (seventh PDPA principle) provides autonomy for data owners to update data and execute legal action in case of personal data misuse.

V. Method

This study employed a qualitative case study to understand and comprehensively describe the social phenomenon under study [29]. Data were collected using interview, document analysis, and observation techniques. Security control elements and the proposed framework were validated based on a case of a public sector agency in Malaysia, known as the National Registration Department (NRD). One-on-one, face-to-face interviews were conducted with seven expert informants at the NRD. These individuals were directly involved with ICT applications (mainly those involving personal data and their sharing with other agencies) and database security of the public sector. The informants and their profiles are listed in Table IV.

The interview agenda was developed based on the research questions and the proposed framework. The agenda was pilot tested with an informant to evaluate the appropriateness of the interview questions. During the interview sessions, the experts were briefed on security control elements. The validated security control elements were refined in the initial framework. The implementation and enforcement processes of the access control system in the NRD office were directly observed. These processes included ID card use among officers and staff, password and biometric use on application systems (particularly at the NRD main counter), and password use for logging on to officer and staff computers. Access control technology, either physical or computerized systems, was also monitored. Important records were also analyzed, they include government documents pertinent to ICT security of public sector, PDPA 2010 (Act 709), ICT security policy for NRD and ISO/IEC 27001:2013, Identification Card System (one of the main systems at NRD counter), and Agency Link-up System (ALIS), one of the systems used for sharing data with statutory body. Documentation for both systems was analyzed from access control implemented on the user who accessed the systems. Data were audio- and hand-recorded and transcribed. They were then organized based on themes and tabulated for subsequent analysis, discussion, and conclusion.

TABLE. IV. INFORMANT LIST

Expert code	Position	Work duration (year)	Expertise (year)
1	Assistant Senior Director (ASD)	12	Application project management (4) ICT security (8)
2	ASD	12	Application project management and development (12)
3	ASD	10	Database (10)
4	ASD	14	Application project management and development (14)
5	ASD	11	Application project management and application (11) ICT security (Internal auditor of ISMS in NRD (5))
6	ASD	14	Application project management (6) Database (5) ICT security (2)
7	ASD	14	Application project management and application (14)

VI. RESULTS

NRD was selected as the case study based on its profile as a government agency that stores data of all Malaysian residents and its role as the main reference for all government, private, and statutory body agencies. NRD also systematically manages information security by obtaining ISO/IEC 27001:2005 and ISO/IEC 27001:2013 certifications. Overall, all the interviewed experts understood the meaning and importance of internal threats at NRD. According to Experts 1, 2, 3, and 4, internal threats include information or technology misuse and document forgery from their own organizations, units, departments, or ministries involving appointed officers, staff, suppliers, or other entities directly involved with NRD.

In addition to ISMS certifications, NRD has also established various procedures and SOPs to ensure ICT security. Numerous experts have confirmed the occurrence of internal threat incidents involving personal data at NRD. According to Expert 4, data from ALIS system were misused and disseminated to an unauthorized third party. Consequently, Expert 4 was interrogated by the Integrity Commission Agency. Furthermore, a server log checks indicated attempts to obtain additional personal data (Expert 3). NRD has strengthened its security mechanism by ensuring non-recurring incidents. The agency also provides policy, guidelines, and briefings on security awareness to all appointed officers, staff, and suppliers. NRD adopts several methods or mechanisms to address internal threats to application and database access involving personal data, namely, internal threats, applications, and database control.

NRD has established access control policy and SOP as procedures to prevent unauthorized use of data or information. A committee was established to approve user ID application for ALIS system. In the case of ID misuse, prevention mechanisms, such as the denial of access and cancellation of IDs and passwords, would immediately take effect. “NRD has a detail access control policy. New or old staff can obtain or remove access upon his relocation or retirement through a specific method” (Expert 7). All experts mentioned background investigations on staff and suppliers involved in ICT projects at NRD; these investigations are conducted to control physical access (human security) to ICT assets. According to Expert 1, “suppliers are obligated to provide service admission letter and Official Confidentiality Act that must be renewed yearly and fill out security clearance under Chief Government Security Officer and obtain approval from NRD security policy”. Experts 2 and 5 supported this statement by stating that NRD practices the compliance principle of ISMS, which requires appointed staff and suppliers to fill out NDA forms.

NRD is yet to establish a specific security policy pertinent to internal threats. However, the agency referred to the highest level and a general ICT security policy [26] in addition to the following: 1) the other policies of the department, including access control procedures on applications, databases, procedure IDs, passwords, and data sharing between the agency and the private sector; 2) meetings and a committee for monitoring access control on issues and NRD problems. These endeavors show the remarkable commitment of NRD management to information security. Furthermore, most of the experts understood the basic PDPA 2010 that was applied to the ALIS system, which involves data sharing with statutory bodies. All appointed officers, staff, and suppliers must comply with all security policies at NRD and sign the recommendation of ICTSP [27] of NRD and the official government act.

Continuous monitoring is implemented to prevent security incidents at NRD, particularly those involving information misuse or leakage. According to Expert 1, risk management has also become the main agenda at NRD because of its inclusion in ISMS and yearly implementation. The other experts also acknowledged the importance of implementing and monitoring risk that is pertinent to internal threats. Expert 1 explained, “Any risk encounter will be mitigated based on the identification of appropriate method and solution alternatives.”

The experts perceived the importance of application control at NRD, which is implemented by ensuring authorization of user access to applications and information. Security and application control are enhanced through system verification, including IDs and passwords, biometrics, and procedures and SOPs pertinent to operational security applications, to ensure smooth daily operation. Despite the importance of cryptography, its application remains costly for the limited budget of NRD.

NRD is the main agency that manages the sensitive data of Malaysian citizens. Therefore, NRD prioritizes database control and has established a specific procedure for its control. The agency tracks database audit trails in cases of problems related to database access. According to Expert 3, “…monthly checking is performed based on the procedure for registering and canceling database access.” An audit trail is a critical component of ISMS. The experts agreed on database cryptography at NRD, as implied by Expert 1, “ISMS NRD is audited by internal and external auditors, involving detailed audit trail check. Auditor check access for active ID and immediate access cancellation for inactive ID for relocated or retired NRD staff.”

All the experts generally agreed with security control elements in the proposed framework based on their clarity and appropriateness to the study context. They also suggested additional elements, namely, ID approval committees and data monitoring data in security policy control and biometrics for IP use, to control user access in application control components.

VII. Discussion

Practice-based research in information security has been advocated to provide insights in actual conduct, challenges, and mitigation approaches implemented in organizations [30]. The validation of the proposed framework indicated the importance on six core and three complementary security controls (information security policy; human resource security control; information security management; operational security; access control; and compliance; risk management; cryptography; and PDPA access principles). The security controls indicated the importance of technical and socio-technical factors, particularly human factors, in ensuring a comprehensive and effective mechanism to protect information. Other studies also corroborate with the significant role of socio-technical aspects in information security [15, 30].

NRD has cultivated a strong security culture through various controls, communication, enforcement mechanisms in a timely, prospective and retrospective, continuous, and comprehensive manner. Despite the absence of a security policy for internal threat, NRD proactively referred to other general, applicable security policies. This is in line with a related study in the Swedish public sector that has no security policy but adopted other practiced information security management approaches [31]. The study associated this workaround as the attitude of knowing how to be “good enough” that adopt, adapt and enhance any available and applicable security measures to the relevant context.

The findings also show that the control mechanism is only effective with continuous monitoring, implementation, compliance, and cooperation from all stakeholders. The concepts are closely related to those of governance, risk, and compliance (GRC) [31, 32].

VIII. Conclusion

This study contributes to the internal threat management discipline, particularly for personal digital data in the public sector. The proposed framework can guide users, specifically managers and officers involved in application, database, and ICT security in the public sector, in protecting organization information from threats or security incidents caused by internal threats. Therefore, risk incidents can be prevented in their early stages to enhance information security. The findings also contribute to organization practice in information security pertinent to access control, a critical security domain in collaborative work environments and various computerized or physical platforms. The framework can serve as a guideline to ensure systematic management of threat control for secured personal data access.

The paper has a number of limitations. Although the scope is limited to one agency, the framework can also be applied in any ministry or public agency because it involves general features for internal threats involving personal digital data. The framework can positively influence government efforts at the information security level to protect personal digital data from any security incident, which can affect data integrity and public sector reputation.

Further research can be conducted on a wider context of local or international public agencies to obtain richer, holistic, and context-specific overview and lesson learned on the subject matter. The research scope can also be extended to information security services for network security monitoring and government security incident management purposes. Further work on all related scope, namely application, database, network security management, and security incident may enhance ICT security in the public sector.

The research scope is also limited to internal threat for protecting digital personal data access only. Therefore, further research on offline data can be conducted as these data are also vulnerable to an internal threat risk. Similarly, the work scope can also be extended to external threat perspective. More work can also be performed on control elements beyond the proposed framework that apply to internal threat in the public sector. The framework components need to be enhanced accordingly in the future based on the requirement, technology, and organizational changes.

The comprehensiveness and appropriateness of the proposed framework in addressing internal threats of personal digital data access in the public sector were validated. The comprehensive framework is applicable in supporting public sector environment and practice in managing internal threat systematically. Based on security policy and procedure and ISMS practice in NRD, the six core security elements are capable of mitigating internal threat for digital personal data access.

Acknowledgment

We thank all study participants from NRD for their collaboration.

References

[1] G. Pavlov and J. Karakaneva. “Information security management system in organization”. Trakia J Sci, vol. 9, no. 4, pp.20-25, 2011.

[2] M.A. Mizhera, R. Sulaiman and A. M.A. Abdalla. “An improved simple flexible cryptosystem for 3D objects with texture maps and 2D images”. J Inf Sec Appl vol 47, pp. 390-409, August 2019.

[3] A. Alwi and K A. Zainol Ariffin. “Information Security Risk Assessment for the Malaysian Aeronautical Information Management System” Cyber Resilience Conference. Putrajaya, Malaysia, November 2018.

[4] A. H. Kashmar, A.K. Hassn and E.S. Ismail. “Hybrid chaotic keystream generation (HCKG) for symmetric image encryption”, J Theor Appl Inf Tech, vol. 97, no. 3, pp. 984-993 1 Feb 2019.

[5] M. Jouinia, L.B.A Rabaia and A. Ben Aissab. “Classification of security threats in information systems”. 5th Intl Conf Ambient Systems, Networks and Technologies, Hasselt, Belgium. June 2014.

[6] P.A. Legg, O. Buckley, M. Goldsmith and S. Creese, S. “Caught in the act of an insider attack: detection and assessment of insider threat”. IEEE Int Symposium on Technologies for Homeland Security, Waltham, USA, 2015.

[7] J. Eggenschwiler, I. Agrafiotis and J.R.C. Nurse. “Insider threat response and recovery strategies in financial services firms”. Comput Fraud Security, vol. 11, pp.12-19, 2016.

[8] A. Price and Y.B. Choi, "Human factors in information security". Int J Comput Inf Tech, vol. 4, no. 5, pp. 833-847. Sep, 2015.

[9] Wan Ismail, W.B. and Yusof, M.M. "Mitigation strategies for unintentional insider threats on information leaks", Int J Secur Appl, vol. 12, no.1, pp. 37-46I, 2018.

[10] Wan Ismail, W.H.B. and Yusof, M.M. "Assessing data leakage prevention for data-in-use", Pacific Asia Conference on Information Systems, Langkawi, Malaysia, July 2017.

[11] X. Shu, J. Zhang, D. Yao, S. Membe, and W.C. Feng. "Fast detection of transformed data leaks." IEEE Trans Inf Forensics Secur, vol. 11, no. 3, pp. 528-542. 2016.

[12] S. Ahmad, S.Z.Z Abidin, N. Omar and S. Reiff-Marganiec. "Managing access control policy from end user perspective in collaborative environment". IEEE Conference on Open Systems, Subang, Malaysia. October 2014.

[13] W.I.W. Sulaiman and M.H. Mambob, "Significance of communication satisfaction model in the context of information management of public sector" Malay J Comm, vol. 30, no. 1, pp. 97-115, 2014.

[14] E. Loukis, and D. Spinellis, "IS security in the Greek public sector". Inf Manage Comput Secur, vol. 9, no.1, pp. 21-31, 2001.

[15] A.I. Al-Darwish, and P. Choe. "Application of a human factors-integrated information security framework to an oil and gas organization". Adv Intell Syst Comput. Vol. 1018, pp. 731-736, 2020.

[16] N. Elmrabit, S.H.Yang, and L. Yang, "Insider threats in information security categories and approaches". 21st Int Conf on Automation and Computing: Automation, Computing and Manufacturing for New Economic Growth, Glasgow, UK. September 2015.

[17] A Sanzgiri, "Classification of insider threat detection techniques". Proceedings of the 11th Annual Cyber and Information Security Research Conference, Tennessee, USA, April,2016.

[18] S. Soltanmohammadi, S.Asadi, and N.Ithnin. "Main human factors affecting information system security". Interdiscip J Contem Res Bus vol. 5, no. 7, pp. 329-354, 2013.

[19] Y. Hashem, H. Takabi, M. Ghasemigol, and R. Andtu, "Inside the mind of the insider: towards insider threat detection using psychophysiological signals". J Internet Serv Inf Secur, vol. 6, no. 1, pp. 20-36, 2016.

[20] Z. Mukhtar and K. Ahmad. "Internal threat control framework based on information security management system. J Theor Appl Inf Tech, vol. 70, no. 2, pp. 316–323, 2014.

[21] ISO/IEC 27001:2013. 2013. International Standard. ISO 27001 "Information technology - security techniques - information security management systems–requirements". https://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf.

[22] Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), "Public sector computer security framework" (PSCSF version 1.0). http://www.mampu.gov.my/images/pengumuman/PSCSF-Versi-1-April-2016-BM.pdf, April, 2016.

[23] N. Baracaldo and J. Joshi. "An adaptive risk management and access control framework to mitigate insider threats", Comput Secur, vol. 39, pp.237-254, 2013.

[24] G. Jabbour, and D.A. Menasce, "The insider threat security architecture: A framework for an integrated, inseparable, and uninterrupted self-protection mechanism". Int Conference on Computational Sc and Eng Vancouver, Canada, pp. 244-251. August, 2009.

[25] Personal data protection department, Malaysia Ministry of Communication and Multimedia. Personal Data Protection Act 2010 (Act 709). Available http://www.pdp.gov.my/index.php/my/akta-709/akta-perlindungan-data-peribadi-2010 2010.

[26] ICT security policy(ICTSP) National Registration Department. MS-NRD-SM-PP-01, 5 February 2015.

[27] A. Munir, L. Sharif, M. Kabir and M. Al-Maimani. "Human errors in information security". Int J Adv Trends Comput Sc Eng, vol. 1, no.3, August, 2012.

[28] F.L. Greitzer and R.E. Hohimer, "Modeling human behavior to anticipate insider attacks." J Strategic Secur, vol. 4, no. 2, pp. 25-48. 2011.

[29] R. K. Yin, "Case study research: design and methods. essential guide to qualitative methods in organizational research, Thousand Oaks: Sage Publications, 2014.

[30] H.A. Hamid, M.M. Yusof, N.R.S.M. Dali, "The influence of security control management and social factors in deterring security misbehavior" Int J Recent Technol Eng, vol 8, no 1, pp 144-150, June 2019.

[31] E. Bergström, M. Lundgren and Å. Ericson, "Revisiting information security risk management challenges: a practice perspective" Inf Comput Secur vol. 27 no. 3, pp. 358-372, 2019.

[32] C. Sillaber, A.Mussmann,and, R. Breu, "Experience: Data and information quality challenges in governance, risk, and compliance management" J Data Inf Qual, vol. 11, no. 2, 2019.

[33] Personal data protection commission Singapore and Privacy Commissioner for Personal Data, Hong Kong. "Guide to data protection by design, for ICT systems", 2019. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Data-Protection-by-Design-for-ICT-Systems-(310519).pdf.