International Journal of Social Science and Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 08 Issue 09 September 2025

DOI: 10.47191/ijsshr/v8-i9-86, Impact factor- 8.007

Page No: 7409-7415

Evaluation Information Security Maturity in Higher Education Institutions Using the Kami Index Based on ISO/IEC 27001: A Case Study at University X

Edy Supriyono[1], Djajasukma Tjahjadi[2], Etin Indrayani[3]

[1]Administrative Staff (Senior Computer Analyst), Institut Pemerintahan Dalam Negeri (IPDN), Sumedang, Indonesia

[2]Lecturer, Information Systems Study Program, LIKMI School of Management Informatics and Computer Science, Bandung, Indonesia

[3]Lecturer, Government Information Systems Engineering Program (TRIP), Institut Pemerintahan Dalam Negeri (IPDN), Sumedang, Indonesia

ABSTRACT: The digital transformation of higher education institutions has introduced new challenges in managing information security. This study evaluates the maturity level of information security at University X using the Information Security Index (KAMI Index) version 5.0, with reference to ISO/IEC 27001:2022. A qualitative descriptive approach was applied through interviews, observations, and document studies. Eight core domains of the KAMI Index were analyzed and mapped to the Capability Maturity Model Integration (CMMI). The findings indicate that most aspects remain at the initial maturity levels (Initial and Repeatable), particularly in governance and risk management. Based on these results, a strategic roadmap and thematic action plan for the 2025–2027 period were formulated to enable continuous improvement. This study provides practical contributions for higher education institutions seeking to strengthen their information security posture systematically and measurably.

KEYWORDS: Information Security, KAMI Index, ISO/IEC 27001:2022, CMMI, Maturity Evaluation, Higher Education

1. INTRODUCTION

Digital transformation has brought fundamental changes in the operations of higher education institutions in Indonesia, starting from academic governance, administration, to public services based on Information and Communication Technology (ICT). In this context, higher education institutions are not only providers of educational services but also managers of sensitive data that include student identities, study results, financial data, and research results. Therefore, the aspect of information security becomes very crucial in maintaining the confidentiality, integrity, and availability of data, as regulated in the CIA triad framework (Confidentiality, Integrity, Availability) (Whitman & Mattord, 2022).

Higher education institutions face increased risks of data leakage and cyber threats due to the digitization of academic and administrative processes (Alshaikh et al., 2018). The implementation of ISO/IEC 27001 in educational institutions has been proven to increase compliance with international standards and reduce incidents of information security breaches (Soomro et al., 2016). Evaluation of the level of information security maturity using models such as CMMI or COBIT helps public organizations in formulating priorities for strengthening security controls (Siponen et al., 2020). The integration of global security frameworks such as ISO with local indicators requires adaptation to remain relevant to institutional contexts (Kayworth & Whitten, 2010). The success of implementing information security greatly depends on governance structures, top management support, and continuous training (AlFayyadh et al., 2021).

Various cases of data leakage that have affected higher education institutions emphasize the weaknesses in implementing information security management systems. Incidents such as the misuse of university subdomains for illegal activities and breaches of academic information systems have occurred in several Indonesian campuses (Ramadhani et al., 2021; CNBC Indonesia, 2023). This phenomenon shows that the maturity level of information security management in many institutions is still low and requires systematic evaluation (Basyarahil, 2017).

In the international framework, ISO/IEC 27001 has become a standard in designing and implementing Information Security Management Systems (ISMS). This standard emphasizes the importance of a risk-based approach, access control, and continuous improvement (ISO/IEC, 2022). In Indonesia, the Information Security Index (KAMI Index) developed by the Ministry of Communication and Informatics has become a national instrument to assess the readiness of agencies for the implementation of information security (Kemenkominfo, 2016).

KAMI Index version 5.0 includes eight main domains, (1) Electronic System Category, (2) Information Security Governance, (3) Risk Management, (4) Security Framework, (5) Information Asset Management, (6) Technology and Security, (7) Personal Data Protection, and (8) Third Party Security. This evaluation becomes stronger when linked to the Capability Maturity Model Integration (CMMI) framework which describes organizational maturity stages from the initial level (Initial) to optimal (Optimizing) (Paulk et al., 1993; ISO/IEC TR 15504, 2004).

Several previous studies have applied a similar approach. Amanda et al. (2021) used the NIST Cybersecurity Framework to measure system security maturity in government agencies. Meanwhile, Rahayu (2021) evaluated the effectiveness of the KAMI Index in the environment of the Department of Communication and Information. However, studies specifically highlighting the implementation of the KAMI Index in higher education institutions are still limited, especially in linking evaluation results with maturity models such as CMMI visually and systematically (Ningrum et al., 2024). This mapping aims to identify the institution's position quantitatively and qualitatively in managing its information security. The analysis process was carried out thematically, by identifying patterns, weaknesses, and potential improvements based on data triangulation from various information-gathering techniques. Data validity was maintained through source and technique triangulation, as well as reconfirmation with informants (member checking) to reduce interpretation bias. With this methodology, the study not only provides a factual picture of the current state of information security but also establishes a strong foundation for strategic recommendations in the form of a roadmap and institutional action plan.

2. RESEARCH METHOD

This study uses a descriptive qualitative approach to evaluate the level of information security maturity at a public university in Indonesia. This approach was chosen because it can describe actual conditions in depth while identifying gaps between ongoing practices and applicable information security standards. Data were collected through in-depth interviews with key informants (ICT unit heads, data managers, and information security staff), direct observation of the systems and procedures used, as well as document studies such as internal policies, audit reports, and technical guidelines. The unit of analysis was selected purposively based on the criteria of having an integrated information system and showing commitment in strengthening data security.

The research instrument refers to the official KAMI Index version 5.0 form which contains indicators such as security policies, information asset classification, risk management, and technical controls. The evaluation was carried out on eight main domains in the KAMI Index: (1) Electronic System Category, (2) Information Security Governance, (3) Risk Management, (4) Security Framework, (5) Information Asset Management, (6) Technology and Security, (7) Personal Data Protection, and (8) Third Party Security.

The results of the assessment of each domain were then mapped into the Capability Maturity Model Integration (CMMI) framework which classifies the maturity level into five levels: Initial, Repeatable, Defined, Managed, and Optimizing (Paulk et al., 1993). This mapping aims to identify the institution's position quantitatively and qualitatively in managing its information security. The analysis process was carried out thematically, identifying patterns, weaknesses, and potential improvements based on data triangulation from various data collection techniques. Data validity was maintained through source and technique triangulation, as well as reconfirmation to informants (member checking) to reduce interpretation bias.

3. RESULTS AND DISCUSSION

The assessment of the maturity level of information security at University X was carried out using the KAMI Index version 5.0 instrument, which was subsequently mapped into the Capability Maturity Model Integration (CMMI) framework. This evaluation aimed to determine the extent of the institution's readiness in managing information security based on the eight main domains. The findings indicate that most domains are still at the initial levels of maturity, which suggests the need for systematic improvements in governance, risk management, and personal data protection.

The evaluation results show that University X is at a maturity level between Level 1 and Level 2 (Initial and Repeatable) in most aspects. Governance, asset management, and staff awareness are the main weak points. Mapping with CMMI reinforces this conclusion. The lack of documented policies, the absence of regular training, and the minimal application of technological controls remain the primary challenges. Based on the GAP Analysis, the priority areas for strengthening are policies, training, and control automation.

The maturity score findings are presented in tables and visual graphs, highlighting weaknesses in governance, risk management, and personal data protection. The analysis explains the influencing internal and external factors. Compared with similar studies, these findings consistently reveal challenges in governance and staff awareness. Practical and theoretical implications are also elaborated.

The following visualization supports the evaluation results obtained through the KAMI Index version 5.0 instrument :

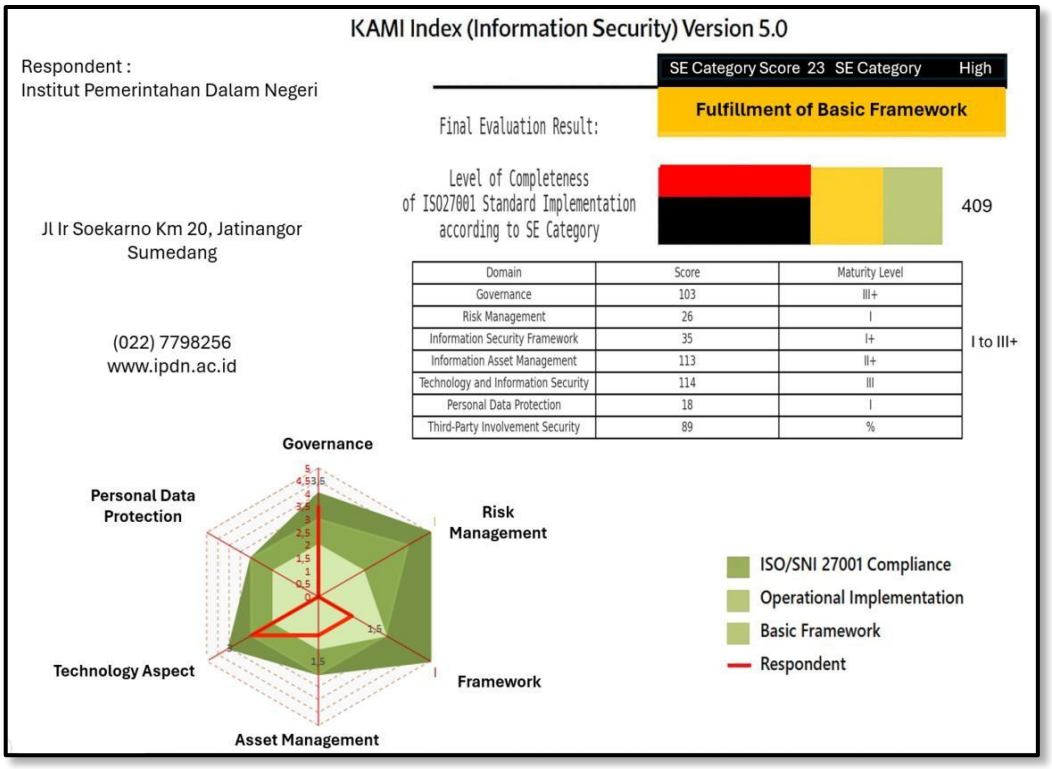

Figure 1. Information Security Readiness Evaluation Dashboard (KAMI Index Version 5.0)

Table 1. Mapping of KAMI Index Scores with the CMMI Maturity Model

KAMI Index Aspect	CMMI Maturity Level	Description
Information Security Governance	Level 3 (Defined)	The information security governance process at the university (X) has been documented and standardized.
Information Security Risk Management	Level 2 (Managed)	The risk management process has been managed and planned, but not yet fully documented.
Information Security Management Framework	Level 3 (Defined)	The information security management framework has been documented and standardized.
Information Asset Management	Level 2 (Managed)	The information asset management process has been managed and planned, but not yet fully documented.
Technology and Information Security	Level 4 (Quantitatively Managed)	The use of technology and information security has been measured and controlled quantitatively.

Source: Research data processing results

This table provides a description of the maturity level of each domain based on the five CMMI levels. Although some aspects, such as Technology and Information Security, have reached Level 4 (Quantitatively Managed), most domains are still at Level 2 (Managed) or even Level 1 (Initial), particularly in risk management and personal data protection. This condition indicates the necessity of establishing formal policies and implementing more consistent standard procedures, as recommended by ISO/IEC 27001:2022 (ISO/IEC, 2022).

As part of the effort to visualize the findings, a mapping of the maturity levels of each information security domain was conducted based on the KAMI Index evaluation results into the five CMMI levels. This mapping aims to provide a comprehensive overview of the relative position of each domain within the maturity spectrum, ranging from the most basic level (Initial) to the highest level (Optimizing). This analysis is important for identifying areas most in need of prioritized policy and technical interventions, while also providing the foundation for formulating a more targeted roadmap for strengthening information security. The following visualization presents the distribution of maturity levels across all assessed aspects. The subsequent chart illustrates the mapping of each component's score into the five CMMI levels. Almost all components remain at the Initial and Repeatable levels.

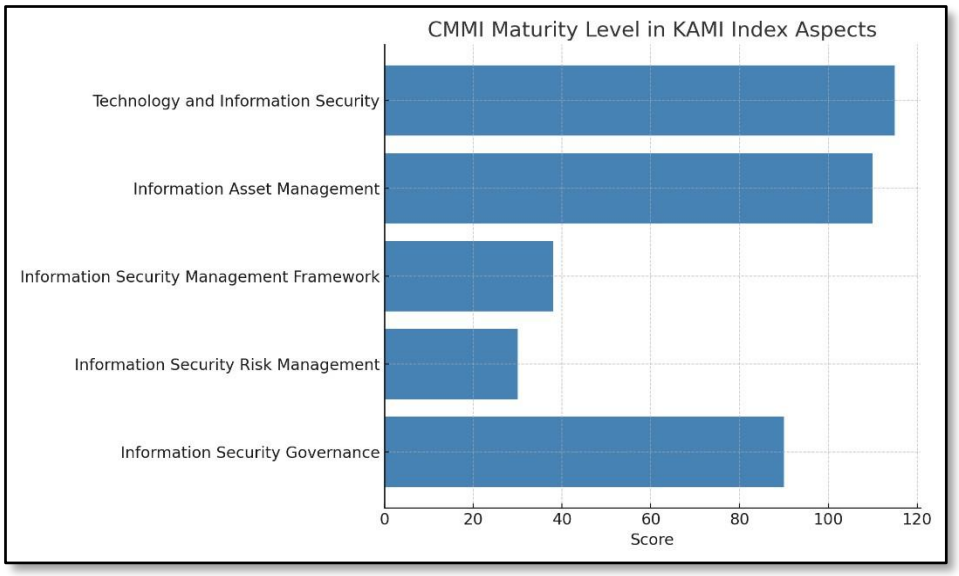

Figure 2. CMMI Maturity Level in KAMI Index Aspects

This figure shows the maturity level of each aspect in the KAMI Index based on the mapping to the CMMI model. It can be seen that the aspects of Governance, Technology and Information Security, and Information Asset Management demonstrate relatively high scores, although not all have reached the maximum maturity level. Conversely, the aspects of Personal Data Protection and Risk Management remain very low and require special attention. This visualization illustrates the urgency of focused improvements in several core domains to ensure that the transformation of information security proceeds comprehensively and in a balanced manner.

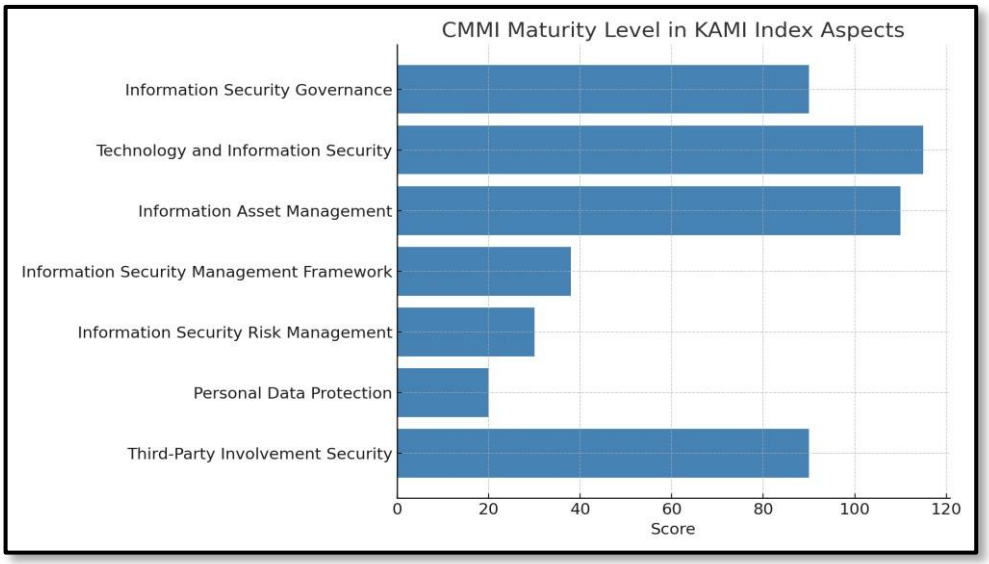

Figure 3. Overview of Initial System and Research Context

Figure 3 above clarifies the distribution of maturity levels across all domains in a visual format. This visualization highlights that although there are initial initiatives in the implementation of security frameworks, practices in the field remain limited to minimal

compliance. This is reinforced by the study of Soomro et al. (2016), which emphasizes the importance of a holistic approach, including policy, technology, and organizational culture aspects, in developing sustainable information security.

These findings are consistent with previous studies by Amanda et al. (2021) and Rahayu (2021), which also highlighted governance weaknesses and the lack of training as the main barriers to the implementation of information security standards. Internal factors such as the limited digital literacy of staff and the absence of regular training were found to be dominant influences. Externally, the lack of specific regulations for the education sector further exacerbates this condition. Therefore, these results serve not only as a basis for reflecting on internal conditions but also as strategic input for formulating a more focused and sustainable roadmap for strengthening information security.

As an important note, the results of the mapping into the CMMI maturity model show that although there are several initiatives in information security management, most domains still operate reactively (Initial level) or in a semi-structured manner (Repeatable level). This condition reflects practices that depend on individuals or specific units rather than being the result of well-standardized and well-documented institutional systems. This is in line with the findings of Soomro et al. (2016), who emphasize the importance of integrating management, technology, and organizational culture holistically to achieve effectiveness in information security. Thus, improvements require not only the adoption of technology or the drafting of administrative policies but also changes in governance structures, leadership patterns, and the strengthening of risk awareness culture at all organizational levels.

Based on the mapping results of the eight information security domains using the KAMI Index version 5.0 and the CMMI framework, it was found that most aspects
of information security management at University X are still at the initial maturity level. This indicates that the efforts carried out so far have not been comprehensively structured and are not yet systematically documented. Therefore, strengthening strategies are needed that address not only technical aspects but also institutional, policy, and human resource development dimensions. The formulation of the following recommendations refers to the principles of continuous improvement and a risk-based approach so that the institution can gradually move toward higher maturity levels and become more resilient to increasingly complex information security threats.

Strategic recommendations are focused on strengthening sustainable information security institutions. The first approach is a medium-term roadmap for 2025–2027, which includes phased stages in drafting information security policies, improving human resource competencies, and utilizing technology for security control. The 2025–2027 roadmap is formulated with annual targets, performance indicators, and the distribution of responsibilities among units. Thematic action plans are arranged according to risk priorities. The focus is placed on policies, human resource training, and the strengthening of technological controls. This roadmap is summarized as a narrative: the initial stage in 2025 will focus on policies and awareness; 2026 on improving human resource competencies and governance; and 2027 on strengthening technical controls and internal audits. If possible, a summary table of the roadmap can also be presented.

Table 2. Information Security Strengthening Roadmap (2025–2027)

Year	Focus Area(s)	Key Targets	ponsible Units	Indicators of Achievement
2025	Policy Development and Awareness	Drafting and formalization of information security policies; Awareness campaigns for staff and students	Governance and ICT Units	Number of formal policies issued; Percentage of staff trained in awareness programs
2026	Human Resource Competence and Governance	Regular training programs; Integration of risk management into institutional planning	HR Division, ICT Units, Academic Administration	Number of training sessions; Evidence of risk management in institutional planning documents
2027	Technical Controls and Internal Audit	Implementation of automated security controls; Conducting periodic internal audits	ICT Units, Internal Audit Division	Percentage of automated controls applied; Number of audit findings resolved

The second approach is a thematic action plan based on the evaluation results of each KAMI Index area. The focus is on improving governance, risk management, personal data protection, and strengthening technical security aspects. These recommendations are designed to align with the principle of continuous improvement, enabling the institution to systematically

progress toward higher maturity levels.

4. CONCLUSION AND RECOMMENDATIONS

This study concludes that the information security maturity of University X remains at a relatively low level, particularly in governance, risk management, and personal data protection. The mapping of the KAMI Index to the CMMI framework confirms that most domains operate reactively or semi-structured, rather than through standardized institutional processes.

It is recommended that the institution adopt a structured roadmap (2025–2027) to gradually strengthen policies, governance, staff training, and technical controls. Future research should assess the effectiveness of these strategies across different higher education institutions in Indonesia.

REFERENCES

1) AlFayyadh, B., Alenezi, A., & Alshammari, R. (2021). The impact of information security governance on information security effectiveness: The mediating role of information security culture. Information & Computer Security, 29(4), 577–592. https://doi.org/10.1108/ICS-11-2020-0175
2) Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). Information security policy: A management practice perspective. Computers & Security, 81, 196–212. https://doi.org/10.1016/j.cose.2018.07.006
3) Amanda, D., Mutiah, N., & Rahmayudha, S. (2023). Analisis tingkat kematangan keamanan informasi menggunakan NIST Cybersecurity Framework dan CMMI [Analysis of Information Security Maturity Level Using NIST Cybersecurity Framework and CMMI]. Coding: Jurnal Komputer dan Aplikasi,11(2), 291–302. https://doi.org/10.26418/coding.v11i2.65088
4) Basyarahil, F. A., Astuti, H. M., & Hidayanto, B. C. (2017). Evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi (KAMI) berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya [Evaluation of Information Security Management Using the KAMI Index Based on ISO/IEC 27001:2013 at the Directorate of Technology and Information Systems Development (DPTSI) ITS Surabaya]. Jurnal Teknik ITS, 6(1), 122–128
5) CNBC Indonesia. (2023). Situs Kampus Disusupi Judi Online, Keamanan Digital Kampus Dipertanyakan. [Campus Website Infiltrated by Online Gambling, Questioning Campus Digital Security] https://www.cnbcindonesia.com/tech/20230403100318-37-428270.
6) Dennis, A., Wixom, B. H., & Tegarden, D. (2015). *Systems Analysis and Design: An Object-Oriented Approach with UML*. John Wiley & Sons.
7) Fahmi, I. (2018). *Manajemen Risiko*. [Risk Management] Alfabeta.
8) ISO/IEC TR 15504. (2004). Information technology – Process assessment – Part 5: An assessment model and indicator guidance. International Organization for Standardization.
9) ISO/IEC. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. International Organization for Standardization.
10) Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technical factors. MIS Quarterly Executive, 9(3), 163–175. https://aisel.aisnet.org/misqe/vol9/iss3/3/
11) Kementerian Komunikasi dan Informatika Republik Indonesia. (2016). Peraturan Menteri Kominfo No. 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi [Ministerial Regulation of Communication and Informatics No. 4/2016 on Information Security Management System]. Jakarta: Kominfo.
12) Ningrum, F. A. S., Riwanto, Y., Pratiwi, I. Y. R., & Fikri, M. A. (2024). Analisis keamanan sistem informasi perguruan tinggi berbasis indeks KAMI [Analysis of University Information System Security Based on the KAMI Index]. JIP (Jurnal Informatika Polinema), 10(3), 441–442. https://doi.org/10.33795/jip.v10i3.5154
13) Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model, version 1.1. IEEE Software, 10(4), 18–27. https://doi.org/10.1109/52.219617
14) Pressman, R. S. (2014). *Software Engineering: A Practitioner's Approach* (8th ed.).McGraw-Hill.
15) Rahayu, S. F., Prawira, D., & Rusi, I. (2021). Pengukuran tingkat keamanan informasi menggunakan metode indeks KAMI (Studi kasus: Dinas Komunikasi dan Informatika Kota Pontianak) [Measurement of Information Security Level Using the KAMI Index (Case Study: Department of Communication and Informatics of Pontianak City)]. Coding: Jurnal Komputer dan Aplikasi, 9(3), 468–477. https://doi.org/10.26418/coding.v9i03.51126
16) Siponen, M., Mahmood, M. A., & Pahnila, S. (2020). Employees' adherence to information security policies: An exploratory field study. Information & Management, 57(2), 103–127. https://doi.org/10.1016/j.im.2019.103120
17) Sommerville, I. (2011). *Software Engineering* (9th ed.). Pearson.
18) Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A

literature review. International Journal of Information Management, 36(2),215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

19) Whitman, M. E., & Mattord, H. J. (2022). Principles of Information Security (7th ed.).Cengage Learning.