



## Bank Security Information Risk Assessment System

Aseel Shaalan Abbas<sup>1</sup> , Sundos A. Hameed Alazawi<sup>2</sup>

### Abstract

Presently, the majority of banking services rely on information technology (IT), hence giving rise to numerous vulnerabilities in IT systems, subpar hardware and software, as well as a lack of attention towards human resources (HR) matters. The utilization of automated systems in banking operations, encompassing transaction processing and financial transfers, is contingent upon the administrative organizational structure of the bank. Consequently, a significant challenge arises in the form of evaluating complex procedures and ensuring their effective execution. The present article presents a system designed to perform a risk assessment for banks, with the objective of safeguarding financial information and security access against theft and potential security attacks that exploit vulnerabilities in information systems and communication networks. The system is comprised of three primary components, namely the Network Environment, Server Environment, and Risks Reporting.

**Keywords:** Information Technology (IT), Information Risk Management, Security Risk Assessment, ISO/IEC 27001

### نظام تقييم مخاطر المعلومات الأمنية للبنك

اسيل شعلان عباس<sup>1</sup> سندس عبدالامير العزاوي<sup>2</sup>

### المستخلص

في الوقت الحاضر، تعتمد غالبية الخدمات المصرفية على تكنولوجيا المعلومات، مما يؤدي إلى العديد من أوجه الضعف في نظم تكنولوجيا المعلومات، والمعدات والبرمجيات الفرعية، فضلاً عن عدم الاهتمام بمسائل الموارد البشرية. ويتوقف استخدام النظم المؤتمتة في العمليات المصرفية، التي تشمل تجهيز المعاملات والتحويلات المالية، على الهيكل التنظيمي الإداري للمصرف. ونتيجة لذلك، ينشأ تحد كبير في شكل تقييم الإجراءات المعقدة وضمان تنفيذها بفعالية. تعرض هذه المادة نظاماً مصمماً لإجراء تقييم للمخاطر بالنسبة للمصارف، بهدف ضمان الحصول على المعلومات المالية والأمن من السرقة والاعتداءات الأمنية المحتملة التي تستغل أوجه الضعف في نظم المعلومات وشبكات الاتصالات. ويتألف النظام من ثلاثة مكونات رئيسية، هي بيئة الشبكة، وبيئة الخوادم، وتقرير المخاطر.

**الكلمات المفتاحية:** تكنولوجيا المعلومات، ادارة مخاطر المعلومات، تقييم المخاطر الامنية، الايزو (27001)

### Affiliation of Authors

<sup>1,2</sup> College of Science, Department of Computer Science, Mustansiriyah University, Iraq, Baghdad, 10052

<sup>1</sup> aseel.shilan@uomustansiriyah.edu.iq

<sup>2</sup> ss.aa.cs@uomustansiriyah.edu.iq

### <sup>1</sup> Corresponding Author

### Paper Info.

Published: June 2024

### انتساب الباحثين

<sup>1,2</sup> كلية العلوم، قسم علوم الحاسبات، جامعة المستنصرية العراق، بغداد، 10052

<sup>1</sup> aseel.shilan@uomustansiriyah.edu.iq

<sup>2</sup> ss.aa.cs@uomustansiriyah.edu.iq

### <sup>1</sup> المؤلف المراسل

### Introduction

Organizations are required to demonstrate a commitment to safeguarding the confidentiality, availability, and integrity of the information under their control. This commitment is essential for effectively managing legal and regulatory duties,

as well as fostering trusted business partnerships. Information security management systems (ISMSs) provide enterprises with enhanced capabilities for addressing information security threats and mitigating cyber-attacks [1] [2]. While numerous methodologies exist for effectively

implementing an Information Security Management System (ISMS) within organizations, the pivotal and resource-intensive aspect of establishing an ISMS is in conducting a comprehensive risk assessment. The objective of this study was to delineate the procedural steps involved in achieving conformity with the International Organization for Standardization (ISO) 27001 (Networks and Communications Part). Subsequently, a comprehensive framework shall be established with the purpose of evaluating the risks associated with banking institutions. The aforementioned risk assessment procedure will be founded upon the principles outlined in the International Organization for Standardization (ISO) 27005. The procedure of evaluating potential risks and implementing requisite configurations to ensure the acceptability of functioning and adherence to information security requirements. Subsequently, the assessments might be observed and printed as reports on a daily frequency [3] [4] In reference to the discourse surrounding the evaluation of risks, it is crucial to explicate the notion of risk and demarcate its diverse classifications within the domain of financial establishments, specifically in the context of banking institutions.

### **1. Risk Types**

In a broader context, risk refers to the likelihood of an occurrence leading to specific negative outcomes, such as physical harm, property loss, organizational harm, and more. When it comes to information security, risk pertains to the potential chance of exploiting vulnerabilities in an asset or set of assets, posing a distinct threat that could harm the organization [1] [2].

### **1.1 Operational risk**

Operational risk is a consequence of various variables, including but not limited to fraudulent activities, errors in processing, disruptions in systems, or unanticipated events. These factors have the potential to impede the institution's ability to deliver its products or services. The aforementioned risk is pervasive throughout the institution's entire range of products and services. The risk level associated with transactions is impacted by the configuration of the institution's processing environment, encompassing the breadth of services offered and the intricacy of the processes and technology employed [5] [6].

### **1.2 Security risk**

The occurrence of a security risk is a result of unauthorized entry into a bank's essential repositories of information, such as the accounting system, risk management system, portfolio management system, and others. Potential attackers encompass a range of individuals, including hackers, unethical vendors, dissatisfied employees, and individuals driven by the pursuit of excitement. The perpetrators are capable of obtaining the necessary authentication details to gain unauthorized access to customer accounts, resulting in financial losses for the bank. Unless explicitly safeguarded, every data or information transmitted via the Internet has the potential to be subjected to surveillance or unauthorized access [6]. [7]

### **1.3 Reputational risk**

The perception of the bank among the general public is commonly referred to as its reputation. This reputation is based on several factors such as the bank's competence, integrity, and reliability, as perceived by stakeholders. inside the given setting,

the proactive management of an individual's reputation assumes a crucial role as a fundamental component inside a bank's comprehensive control structure. Additional factors that contribute to reputational risk encompass the occurrence of losses encountered by comparable institutions providing analogous services, which may lead customers to regard other banks with scepticism. Moreover, targeted assaults on a bank, such as the dissemination of false information about the bank's offerings by hackers, or the occurrence of a virus that disrupts the bank's systems, can result in issues pertaining to the integrity of the bank's systems and data, among various other factors [8] [9].

#### **1.4 Legal and compliance risk**

Relates to the possibility of non-compliance with legal or regulatory obligations. The aforementioned hazards are intricately linked to electronic banking and have a tendency to increase in magnitude as its utilization proliferates. The complexity of providing electronic services to various countries is heightened due to the absence of a single international legal framework. In contrast, each nation implement and uphold their respective regulations, hence presenting a formidable obstacle for a financial institution to consistently adjust its offerings and stay abreast of the legal frameworks within each specific jurisdiction [8] .

An additional facet of legal risk is to the protection of clients' personal data. Insufficient management by bank personnel or intentional external intrusions might subject a bank to substantial legal obligations. The utilization of electronic banking by financial institutions is anticipated to entail increasing legal risks, primarily due to the uncertainties surrounding the overarching legal

structure and specific regulatory provisions that govern transactions conducted over an open electronic network, such as the internet [10] [11].

#### **1.5 Money laundering risk**

In the realm of financial misconduct, wrongdoers employ a multifaceted approach to obscure the origins of illicitly obtained funds by intermingling them with lawful financial activities. These funds typically emanate from unlawful undertakings and may subsequently be channeled into further illicit pursuits, such as the support of terrorist operations. Considerable research has been dedicated to the identification and prevention of financial wrongdoing, encompassing conventional statistical methodologies as well as more contemporary approaches rooted in machine learning [1] [3].

#### **1.6 strategic risk**

The field of E-banking is relatively new, leading to a potential lack of comprehension among senior management regarding its possibilities and consequences. In some cases, individuals possessing technological expertise but lacking a deep understanding of banking can end up spearheading these initiatives. Consequently, E-initiatives may emerge within organizations in a disjointed and fragmented manner [4] [5].

#### **1.7 Other risk**

Risks such as credit risk, liquidity risk, interest rate risk, and market risk, typically associated with conventional banking, can also manifest in the context of electronic banking and electronic money activities. Nevertheless, the potential consequences of these risks for banks and regulatory agencies may vary in terms of severity in comparison to operational, reputational, and

legal concerns. The aforementioned differentiation holds significant relevance for banks engaged in diverse banking operations, in contrast to banks or their affiliated entities that concentrate exclusively on electronic platforms[6] [9].

## 2. Literature Survey

In the recent period, due to the importance of risk assessment in commercial and banking institutions in particular, researchers and authors interested in risk assessment and management have carried out works related to the subject of this manuscript. The following is a number of those works.

- N. Legowo and Y. Juhartoyo (2022) [12].they conduct a risk assessment, determine the level of maturity of the information technology security system using a checklist from Annex A of ISO 27001, which contains 11 domains and 39 control objectives, and conduct a risk assessment of information technology assets, as well as provide recommendations for controlling the risk level. Their data is collected through observation and interviews based on questionnaires. The results of the condition of the security system technology's gap analysis and the current maturity level has reached 75%, according to information gathered using a checklist based on Annex.
- D. Vitkus et al. (2019) [6]., This study proposes a solution to the problem by introducing a method for developing an automated knowledge base in the field of expert systems. The method involves segregating the ontology subset, specifically the Web Ontology Rule Language (OWL RL), into Resource Description Framework (RDF) triplets. These triplets are then turned into Rule Interchange Format (RIF). Subsequently, the knowledge base that was generated underwent validation through the execution of comparative risk analysis within a representative company.
- Within the domain of information security research, the ISO 27001 standard assumes a significant role as a beneficial point of reference for the implementation of measures aimed at safeguarding information. The present study investigates the management of information security risks specifically inside government bodies, as referenced by Study 21. This statement delineates the formulation of security control objectives within the larger framework that includes the identification of information assets, risk assessment, and risk mitigation. Furthermore, the study integrates the methodology of the System Security Engineering Capability Maturity Model (SSE-CMM) throughout the evaluation phase to evaluate the efficacy of implementing these standards.
- The research conducted in reference [10]. involved a comprehensive evaluation of information security risks, specifically focusing on assessing the potential risks associated with information assets and their implications for academic information systems. The study employed a methodology that calculated the value of these assets and assessed the associated risks, utilizing criteria aligned with the principles found in the ISO 27001 standard, particularly focusing on confidentiality, integrity, and availability (CIA) aspects.
- ISO/IEC 27001:2013 The document serves as a complete framework that delineates the necessary steps for establishing, implementing,

maintaining, and continuously enhancing an Information Security Management System (ISMS) within the organisational context. Furthermore, it includes a set of standards for evaluating and reducing the potential threats to information security that are in line with the goals of the organisation. The provisions delineated in ISO/IEC 27001:2013 are of significant importance, as they are deliberately designed to have a wide scope and be relevant to organisations across all sectors, regardless of their size or kind. The aforementioned standard is highly regarded and holds global acknowledgement as a reference point for security protocols [11].

- A company that has obtained ISO 27001 The implementation of certification processes has the potential to significantly alleviate the adverse consequences associated with data breaches. It is essential to construct a robust incident response system for information security in accordance with the criteria set forth by ISO 27001. This necessitates the implementation of a well-organized system to expeditiously identify and mitigate any potential risks to the security of information. In light of the persistent occurrence of cyberattacks, it is imperative to promptly detect and identify them at their nascent phases. In the specific instance of the data breach that occurred at Target stores, there was a notable delay of over one week in the detection of the attack. Had the attack been detected earlier, the magnitude of data exposure would have been mitigated, so minimising the repercussions on clientele. The potential utilisation of an information security incident response system may have significantly contributed to the timely identification and alleviation of the attack [12].
- Risk assessment should not be limited to present concerns, but should also consider potential future obstacles, including emerging systems and innovations, both existing and predicted. The use of risk assessment facilitates a thorough understanding of the organisation and its operations. The risk assessment team strives to comprehend the interaction between systems and procedures, allowing the organisation to identify shortcomings in its operations. Nevertheless, it is imperative to underscore the importance of employees tasked with performing the risk assessment to possess a thorough and expansive outlook, along with substantial expertise across the entirety of the organisation[13] [14].
- ISO/IEC 27005 The standardised technique provided offers a means to undertake information security risk management within an organisation, serving as a crucial element of an Information Security Management System (ISMS) [3]. The aforementioned standard possesses a universal applicability, as it offers a comprehensive framework for the process of risk management that can be utilised by organisations operating in diverse sectors and industries[15].
- A study was undertaken to analyse the obstacles impeding the adoption of information management systems. The findings of the study indicate that the successful execution of the implementation process is contingent upon the active involvement of all individuals and groups with a vested interest in the project. The

recommended approach entails the involvement of senior management, ensuring consistent communication of employee guidelines, conducting regular assessments of the implementation of Information Security Management Systems (ISMS), promptly disseminating updates to employees, transparently communicating roles, responsibilities, and authority related to ISMS to employees on an ongoing basis, formulating implementation work plans for information security systems that are shared with staff, and frequently communicating information security policies and objectives to employees. [16].

- This article aims to address the issue of selecting an appropriate methodology for assessing and managing information security threats. This is achieved by giving a collection of evaluation criteria that are systematically

categorised into four distinct groups. The subsequent step involves performing a comparison analysis of ten well-established risk assessment methodologies. This allows organisations to evaluate and select the most suitable methodology that matches with their specific objectives. The primary objective is to provide a comprehensive understanding of the process of selecting a methodology based on the aforementioned criteria [17].

### 3. Proposed System

The system consists of main parts: Network Environment, Server Environment, and Risk Reporting. As shown in Fig. (1), the components of are interconnected to establish the proposed system a risk assessment system for banking information (RAFSBI).

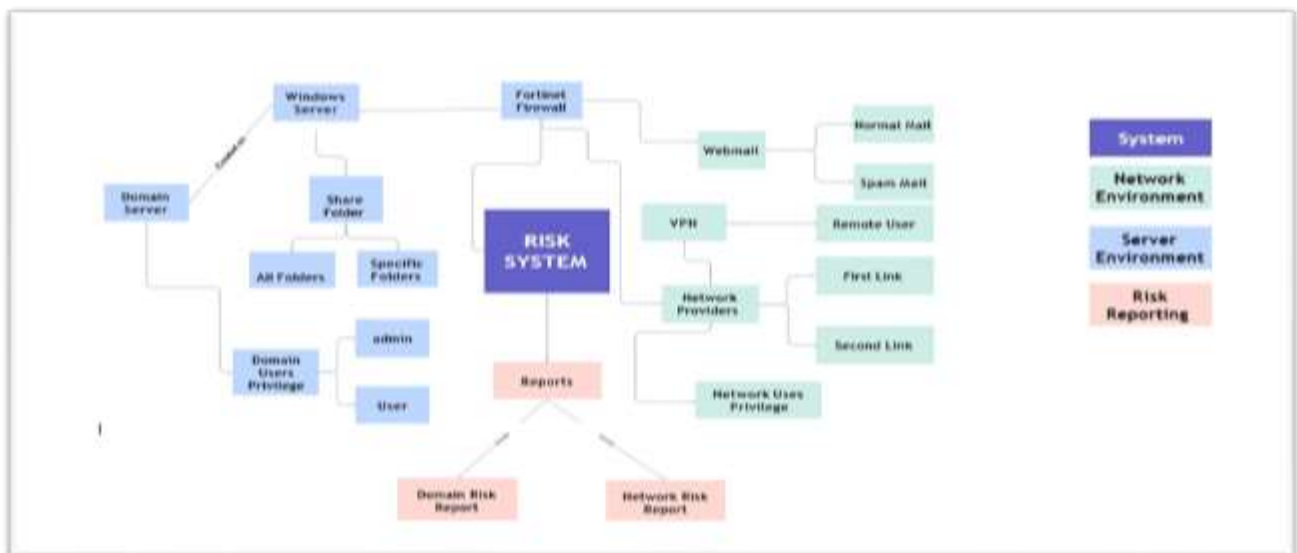


Figure (1): The General Structure of the (RAFSBI). Proposed System

By establishing a risk management process in accordance with ISO/IEC 27005, organizations enhance the effectiveness of their Information

Security Management Systems (ISMS), effectively address information security risks, and establish sound information security risk management




procedures. By creating an electronic system that derives the idea of creating it from expert systems, it is a computer-based system that consists of multiple components. Risks are calculated for all these parts and inputs to the network, where the data set for this system is the data of employees in the financial institution (the bank) and all devices such as computers, servers, banking system devices, etc., including the Internet, are considered as assets of the institution.

The utilization of a virtual machine (VM) as the operating system will facilitate user access to the electronic system. A virtual machine (VM) is an emulated environment that functions as a virtual computer system, encompassing its own central processing unit (CPU), memory, network connectivity, and storage. The virtual environment is created within a physical hardware system, which can be situated either on-site or off-site. The hypervisor, a software component, plays a crucial role in ensuring the proper functioning of a virtual machine (VM) by isolating its resources from the underlying hardware and allocating them appropriately. Virtual machines (VMs) facilitate the simultaneous operation of numerous separate operating systems on a solitary computer. Each of these operating systems functions within the virtual machine in a manner consistent with its regular operation on the underlying hardware. As a result, the user experience within the virtual machine closely emulates that of executing an operating system on tangible hardware, providing an almost indistinguishable real-time experience. Subsequently, commence the implementation of ISO 27001 controls, followed by the undertaking of a risk assessment utilizing OWASP (Open Web Application Security Project). There are multiple methodologies available for the purpose of

performing risk assessments. The technique presented in this document is based on well-established approaches and has been specifically designed to improve application security. The risk associated with an application can be quantified using the OWASP approach, as expressed in Equation (1):

$$\text{Risk} = \text{Likelihood} * \text{Impact} \quad (1)$$

The combined assessment of likelihood and impact is used to determine an overall severity rating for this risk. This involves categorizing both likelihood and impact as low, medium, or high on a scale ranging from 0 to 9, which is divided into three sections [18] :

1. 0 to < 3	
2. 3 to < 6	
3. 6 to 9	

After conducting an evaluation of all network inputs and parts of the system, all previous partial evaluations are collected and a complete comprehensive risk evaluation is conducted in two parts:

- The first part is concerned with assessing individuals' risks for information security based on the domain server, as all individuals' data will be stored in the domain server, and a special assessment report for this part will be printed.
- As for the second part, it is concerned with evaluating the risks of network information

security, based on all direct inputs to the network, as well as printing a report on this evaluation for this part.

#### 4. Conclusion

Risk management poses a significant challenge for organizations, particularly in the context of IT governance and computer security. Information security encompasses challenges related to operational IT assets and also has a profound impact on the organization as a whole [19]. This study explores the implementation of a risk assessment system for banking information. This is crucial because security threats can potentially harm information technology assets and subsequently affect the organization.

The results of this inquiry emphasize the need of implementing a framework for evaluating risks inside an organization. The accomplishment of this objective is attained by the implementation of an information security risk assessment procedure that conforms to the stipulations specified in ISO/IEC 27001. [20]. Risk assessment serves as a foundational element of comprehensive risk management. It entails an examination of the likelihood of risk occurrences and an assessment of the potential magnitude of their impact [21].

To implement this evaluation process, the study employs the OWASP (Open Web Application Security Project) methodology. OWASP is founded on the calculation of the probability and potential consequences of various risks for an organization [22]. The outcome of this evaluation process yields regular reports that are furnished to the organization. These reports provide critical insights into the level of security threats faced by the organization on a day-to-day basis, thereby

enabling proactive measures to mitigate these threats and prevent potential harm to the organization [23] [24].

#### References

- [1] Solanki VS. Risks in e-banking and their management. *International Journal of Marketing, Financial Services & Management Research*. 2012;1(9):164-78.
- [2] Huang J, Huang Z, Shao X. The risk of implicit guarantees: Evidence from shadow banks in China. *Review of Finance*. 2023;27(4):1521-44.
- [3] Leo M, Sharma S, Maddulety K. Machine learning in banking risk management: A literature review. *Risks*. 2019;7(1):29.
- [4] Saputra I, Murwaningsari E, Augustine Y. The Role of Enterprise Risk Management And Digital Transformation On Sustainable Banking In Indonesia. *Neo Journal of economy and social humanities*. 2023;2(1):17-30.
- [5] Lauren EA. The Fourth Industrial Revolution in Banking Sector: Strategies To Keep Up With Financial Technology. Available at SSRN 4049913. 2021.
- [6] Vitkus D, Steckevičius Ž, Goranin N, Kalibatiėnė D, Čėnys A. Automated expert system knowledge base development method for information security risk analysis. *International journal of computers, communications and control*. 2019;14(6):743-58.
- [7] Duho KCT, Duho DM, Forson JA. Impact of income diversification strategy on credit risk and market risk among microfinance institutions. *Journal of Economic and Administrative Sciences*. 2023;39(2):523-46.



- [8] Haris L, editor Risk Assessment on Information Asset an academic Application Using ISO 27001. 2018 6th International Conference on Cyber and IT Service Management (CITSM); 2018: IEEE.
- [9] Velasco J, Ullauri R, Pilicita L, Jácome B, Saa P, Moscoso-Zea O, editors. Benefits of implementing an isms according to the ISO 27001 standard in the Ecuadorian manufacturing industry. 2018 International Conference on Information Systems and Computer Science (INCISCOS); 2018: IEEE.
- [10] Hsu C, Wang T, Lu A, editors. The impact of ISO 27001 certification on firm performance. 2016 49th Hawaii International Conference on System Sciences (HICSS); 2016: IEEE.
- [11] Zio E. The future of risk assessment. *Reliability Engineering & System Safety*. 2018;177:176-90.
- [12] Legowo N, Juhartoyo Y. Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001. *J Syst Manag Sci*. 2022;12:181-99.
- [13] Saleh I, Abu Afifa M. The effect of credit risk, liquidity risk and bank capital on bank profitability: Evidence from an emerging market. *Cogent Economics & Finance*. 2020;8(1):1814509.
- [14] Marhavalas PK, Tegas MG, Koulinas GK, Koulouriotis DE. A joint stochastic/deterministic process with multi-objective decision making risk-assessment framework for sustainable constructions engineering projects—A case study. *Sustainability*. 2020;12(10):4280.
- [15] Putra SJ, Gunawan MN, Sobri AF, Muslimin J, Saepudin D, editors. Information Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company. 2020 8th International Conference on Cyber and IT Service Management (CITSM); 2020: IEEE.
- [16] Tatiara R, Fajar A, Siregar B, Gunawan W, editors. Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001. *Journal of Physics: Conference Series*; 2018: IOP Publishing.
- [17] Gritzalis D, Iseppi G, Mylonas A, Stavrou V. Exiting the risk assessment maze: A meta-survey. *ACM Computing Surveys (CSUR)*. 2018;51(1):1-30.
- [18] Riadi I, Raharja PA. Vulnerability analysis of E-voting application using open web application security project (OWASP) framework. *International Journal of Advanced Computer Science and Applications*. 2019;10(11).
- [19] Amraoui S, Elmaallam M, Bensaid H, Kriouile A. Information Systems Risk Management: Litterature Review. *Comput Inf Sci*. 2019;12(3):1-20.
- [20] Kitsios F, Chatzidimitriou E, Kamariotou M. The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability*. 2023;15(7):5828.
- [21] Kuzminykh I, Ghita B, Sokolov V, Bakhshi T. Information Security Risk Assessment. *Encyclopedia*. 2021;1(3):602-17.
- [22] Shameli-Sendi A. An efficient security data-driven approach for implementing risk assessment. *Journal of Information Security and Applications*. 2020;54:102593.
- [23] Haji S, Tan Q, Costa RS. A hybrid model for information security risk assessment. *Int j adv*

trends comput sci eng. 2019(ART-2019-111611).

- [24] Shaikh FA, Siponen M. Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*. 2023;124:102974.