

Proposed model for data protection in information systems of government institutions

Haifaa Jassim Muhasin, Ali Yahya Gheni, Hiba Adil Yousif

Department of Computer Science, Faculty of Education for Pure Science, College of Education for Pure Science/Ibn Al-Haitham, University of Baghdad, Baghdad, Iraq

Article Info

Article history:

Received Feb 25, 2022

Revised Apr 16, 2022

Accepted May 23, 2022

Keywords:

Administration

Awareness

Information systems

Organizational

Policy

Security

ABSTRACT

Information systems and data exchange between government institutions are growing rapidly around the world, and with it, the threats to information within government departments are growing. In recent years, research into the development and construction of secure information systems in government institutions seems to be very effective. Based on information system principles, this study proposes a model for providing and evaluating security for all of the departments of government institutions. The requirements of any information system begin with the organization's surroundings and objectives. Most prior techniques did not take into account the organizational component on which the information system runs, despite the relevance of this feature in the application of access and control methods in terms of security. Based on this, we propose a model for improving security for all departments of government institutions by addressing security issues early in the system's life cycle, integrating them with functional elements throughout the life cycle, and focusing on the system's organizational aspects. The main security aspects covered are system administration, organizational factors, enterprise policy, and awareness and cultural aspects.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Haifaa Jassim Muhasin

Department of Computer Science, Faculty of Education for Pure Science

College of Education for Pure Science/Ibn Al-Haitham, University of Baghdad

Baghdad, Iraq

Email: haifaa.j@ihcoedu.uobaghdad.edu.iq

1. INTRODUCTION

The development of information systems infrastructure is critical for improving government work, but the main issue is security threats and concerns. These are service and infrastructure concerns, as the loss of government data, as well as violations of citizens' privacy and confidentiality, is a major challenge for government institutions [1], [2]. The primary goal of the research is to develop and implement a model for providing and evaluating information security in organizations. In recent years, government institutions' research into the development and construction of secure systems has been extremely effective. Some contributions focused on integrating security aspects, particularly access control mechanisms, during the implementation phase, whereas others focused on identifying and analyzing security requirements [3]. However, there is no way to address the entire issue of security requirements and their transformation throughout all stages of an information system's life cycle.

The performance of work in the institution is dependent on important and decisive factors, such as availability, efficiency, security, and quality of information, service function, and transparency, all of which contribute to improving the institution's performance [4]. The development and increasing use of mobile

devices and the Internet to access data in sensitive government institutions makes them an appealing target for cybercriminals. As a result, the adoption of advanced technology in institutions typically necessitates specialized training and awareness for working people to acquire new skills [5]. However, the implementation of information and communication technologies (ICT) in government institutions has created numerous challenges, particularly privacy concerns and weaknesses related to the ability to provide citizens with access to large amounts of data [6]. There are also concerns about access to enterprise information systems and the risk of unauthorized access from within the organization [3].

Security is an important aspect of information systems. Where security methods have evolved in a manner similar to that of information systems. Security and information systems share goals, means, and challenges, so they rely on risk review and analysis to determine acceptable information system protection. Interest is growing in methods and models for understanding the security requirements for information systems. Through this interest, it appears that information system security methods cannot achieve the required results unless they are integrated with methods for developing public information systems [7], [8]. The convergence of the two tracks results in the development of clear methods for providing security and safety controls for information systems. According to [9], [10], information security issues are considered management's responsibility because they affect the company's market position, and this study advises organizations to take a more volatile approach to information. Security management entails senior management involvement, human resource management, the development and implementation of an information security policy, information security awareness and training, and the involvement of strategic decision makers [11]. Research by Crowley [12] discusses information system security training and educational dynamics. This paper also presents a graduate-level information system security specialization developed using this information. The purpose of the paper [13] is to identify and prioritize the main issues that local government chief information officers are dealing with, or believe they will be dealing with in the near future, in the field of information systems security management.

A researcher investigated the non-research fields of human resources information system (HRIS) and HR Electronic Security in [14]. By outlining the fundamentals of information security and how it relates to businesses. Issues concerning the human resources information system and electronic human resources security were discussed, and instructions for dealing with these security issues were provided via the research form. Concerns about the security of the human resources information system must be addressed because the use of the human resources information system, electronic human resources, and similar enterprise systems will only increase. The researchers proposed an information security assessment plan in [15], taking into account academic institution expectations and related regulatory requirements. The primary goal of this plan is to provide an internal assessment and role-based response system, rather than just a checklist of security metrics. The proposed scale addresses the specific needs of three types of organizations: small, medium, and large. This approach drives iterative implementation and serves as a stepping stone for small businesses to protect their valuable information assets.

The proposed method in [16] enables companies associated with information technology or on which it is based to implement information security management system (ISMS) related to them, using appropriate standards in this field and some information security management system standards. This method aids in the identification of related weaknesses and threats, as well as the assessment of risks and the provision of appropriate treatment methods. This method allows large information technology companies to establish an information security management system. The goal of [17] is to provide an analytical description of methods for analyzing and designing the security of information systems. This research deals with the methods by comparing them to the known methods of developing information systems, and in this way it is possible to understand the existing techniques for providing secure computing resources, identify the methods of developing systems, and learn about new research methods.

The research study by Sillaber and Ruth [18] aims to validate stakeholder participation in the early stages of management process analysis of risks related to information system security, as well as how users' awareness of the style and business process model affects the risk management process for information system security, particularly the security requirements in terms of number and accuracy. This paper responds to requests for user participation in information system security-related processes, as well as validates findings from several case studies conducted within the organization under investigation. It is necessary to focus on IT governance, which includes leadership, organizational structure, and processes, to ensure that the IT organization supports and expands the organizational strategies and goals [19]. In this paper, we will present a proposed model for a security information system for a government institution, taking security issues into account early in the system's life cycle and integrating these issues with functional aspects throughout the system's life cycle. Where the functional requirements are integrated and include social, awareness, informational, and organizational aspects.

2. METHOD

There are numerous challenges and obstacles associated with data protection in government institutions that must be addressed early in the system life cycle and integrated with the functional aspects of the system life cycle stages [6]. It can be classified into the following categories:

- a. Technical issues: these are issues with the organization's infrastructure, security mechanisms, and data integrity.
- b. Policy issues: defining and providing services, defining responsibilities, and defining the institution's overall policy.
- c. Awareness and cultural challenges: this includes issues such as user distrust, threats to confidential data and privacy, and licensing and liability limitations.
- d. Legitimacy: it represents issues associated with network crimes and a lack of information technology laws.

Every government's primary goal is to provide the best services possible in order to establish efficiency and quality of performance [20], [21]. The proposed model for providing enterprise information systems security demonstrates that information security is critical and is addressed from the system's inception. Software and hardware security, workstation security, personnel and physical issues are all examples of security measures. Organizational measures such as data security, procedures, and administrative aspects are also critical. The second factor is the institution's policy. The final aspect is related to awareness and culture in terms of information security within the organization, as well as spreading security awareness among employees. As shown in Figure 1 depicts the information system security factors in the proposed model. The model for data protection in government information systems is depicted as shown in Figure 2.

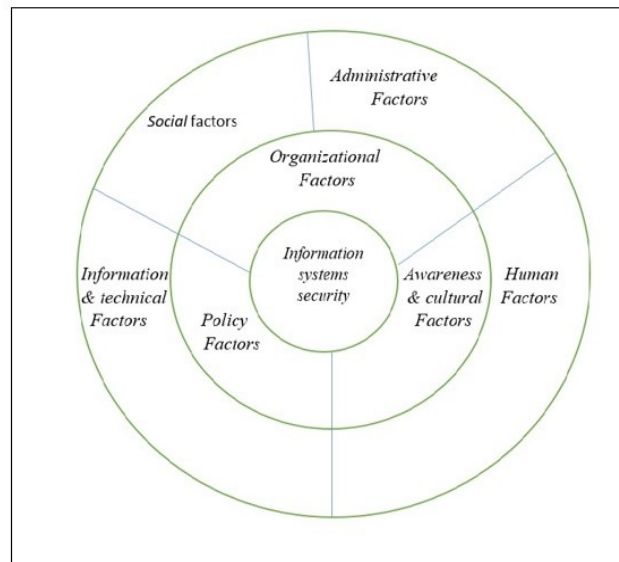


Figure 1. Factors of the proposed information systems model

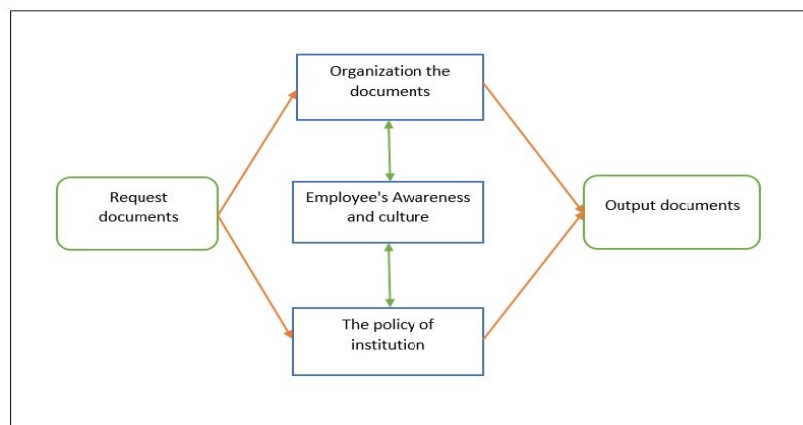


Figure 2. The model of data protection in information systems of government institutions

2.1. Organizational and administrative factors

Information Security Management is a management system integrative philosophy for continuously improving the quality of information security operations and implementing high-quality information security within the organization [22]. All members of the organization (Head of Information Department (HID), IT staff, end users) are involved in improving processes related to the quality of information security. To achieve these goals, an assessment plan must be designed based on the needs of the organization by defining the main responsibilities required for system management, and a reporting approach is used where these reports help reduce the time specified for responding to any emergency event where the appropriate responsible for planning and implementation participates [23]. Reduced response time is critical for effective security management. There are two categories of organizational and administrative factors:

- a. social factors: these include
 - Create and implement a method to ensure the quality of information security within the organization. Throughout the information security lifecycle, which includes risk management, process measurement, process improvement, and process management.
 - Develop a comprehensive security strategy for technology and operations. An effective, high-quality information security program necessitates the use of technology, processes (policy, standards, and procedures), and people.
 - Developing training programs to improve information security. Because information security is everyone's responsibility, it eliminates barriers between IT and other departments.
- b. administrative factors, such as
 - Managing, developing, and implementing information security methods within the organization. Organizations should improve the quality of information security to support the protection of sensitive data, employee and customer privacy, and business and business survival objectives.
 - Creating and implementing a mechanism for assessing information security in the organization. The development of the evaluation mechanism is dependent on the assessment of the organization's risks. The organization must identify critical risk factors and indicate the level of exposure.
 - Controlling internal and external threats. It is the analysis of attack behavior and the provision of proactive advice to improve enterprise security. Specify the level of potential exposure.

2.2. Institution policy factor

Develop and implement a quality information security policy within the organization through strong policies to improve the organization's quality. Policies for information system security are developed, and organization members are informed of their responsibilities for protecting their organization's information systems. Information system security policies establish the foundation for acquiring, configuring, and auditing information systems for policy compliance [11].

Official information protection policies include the creation of a specialized information protection department, the appointment of a person responsible for information protection (the head of information security), and an increase in information protection personnel [24]. The main factors for institutional policy are informational and technical factors, which include the following:

- a. Implementation of an effective and high-quality information security program throughout the information security system's life cycle.
- b. Internal and external threat risk analysis
- c. A policy that assists in the design and implementation of an effective information security system that meets the needs and objectives of the organization.

The areas concerned with security measures for information system programs are as follows: (organizing the user account, managing and generating passwords, managing and controlling access control, using encryption methods, organizing and managing security records).

2.3. Awareness and cultural factors

Develop information security training and awareness programs. Training and awareness must be prioritized for the success of the information security program, especially training the organization's information technology staff and users on the security policy. In terms of the procedures and techniques used, as well as the various administrative and operational controls required and available to secure the institution [25]. Information security and organizational culture are both important factors to consider. At the enterprise level, information security is not limited to specific employees; however, it is necessary to create an organizational culture that emphasizes the importance of information security and raises enterprise awareness [9], [26]. Human factors are the most important for raising awareness and cultural factors, and they include the following:

- Creating and implementing a culture of concern for the quality of information system security among the institution's employees.
- Raising employee security awareness.
- Develop methods for securing the organization's technology, procedures, policies, and people, which are the fundamental components of an effective information security program.
- Develop training and awareness programs for the institution's employees, particularly those working in the field of information systems security.

The model for data protection in government information systems with factors is depicted in Figure 3.

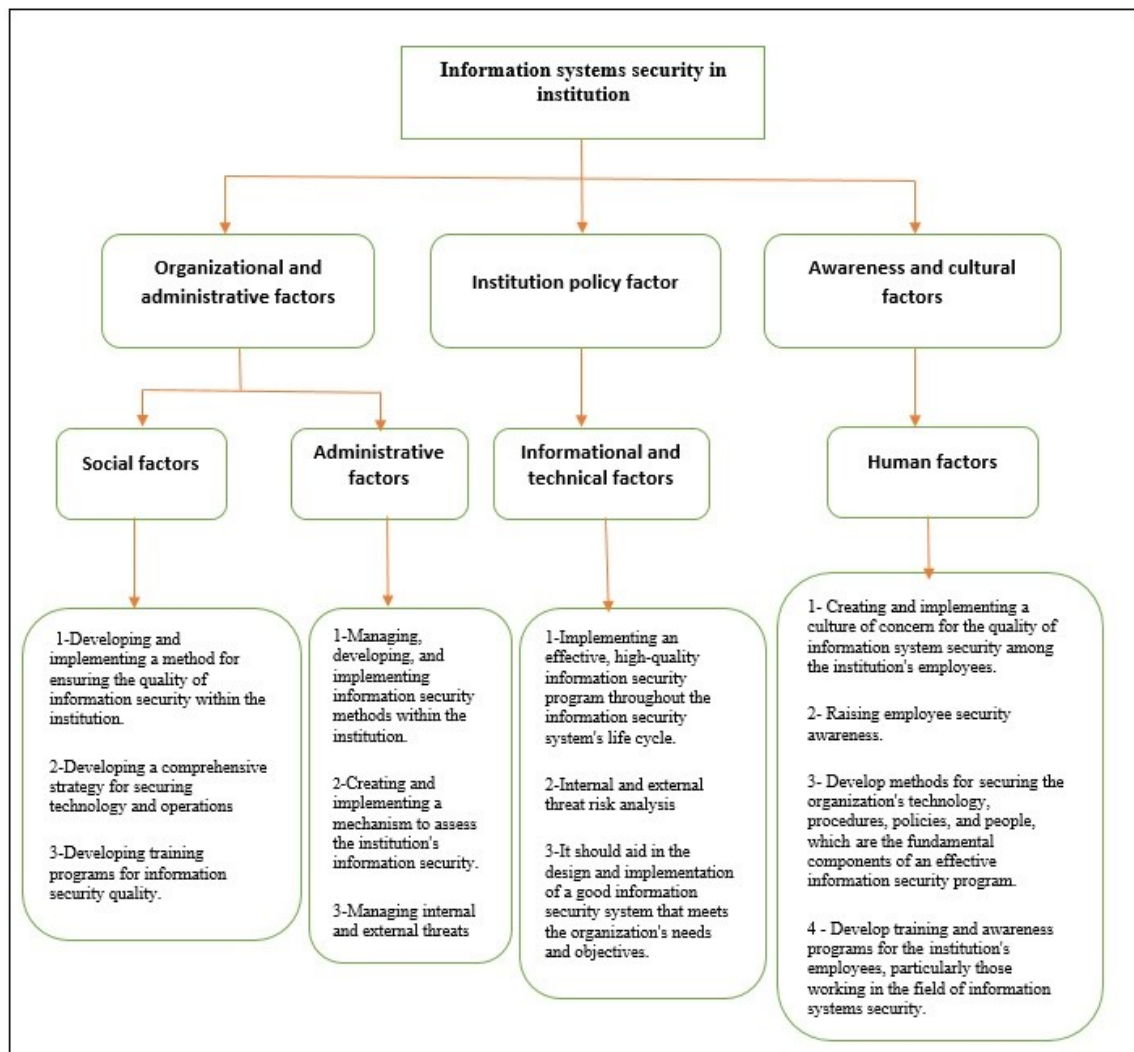


Figure 3. Data protection in information systems of government institutions model with factors

3. CASE STUDY

Consider the information system for the issuance of graduate documents in the Registration Division of a college within the University of Baghdad. We note that all of the factors required to protect information in the system from organizational and administrative aspects, as well as the work policy available in the Registration Division's information system, particularly data related to degrees and related documents, in addition to raising awareness and awareness of workers in this field, are all required. Regarding the security aspect of ensuring the integrity of data related to graduates from degrees and personal data that must be available to ensure that the information system operates correctly and securely.

This paper focuses on the process of issuing a graduation certificate for a college graduate. For example, the process begins with the applicant completing an electronic form via the form link provided by the Registration Division and attaching a copy of the wage payment receipt received from the Accounts

Division, which will be delivered later upon review by the Registration Division, as well as delivering personal photos with the required documents. The form is reviewed by file staff to ensure that the file is complete and that there are no missing documents. The document is then organized by the competent employee. When there are missing documents in a student's file, he is notified of their completion via e-mail or phone call. After the document has been organized, printed, and signed by the concerned employee, the information is checked with the electronic graduate system, and after verifying its authenticity, it is sent to the Director of Registration for checking and signing, then to the Assistant Dean for signature, and finally to the Dean for signature. Finally, it is returned to the registry to be assigned a number and forwarded to the university via letter for certification.

We can see from the previous steps regarding the issuance of an average document for a college graduate that the steps concerning organization and auditing are among the administrative and organizational steps concerning graduates, which represent functional factors. The work policy of the Registration Division, as well as the measures taken to maintain information confidentiality, are all in accordance with this policy, which represents non-functional factors. As shown Figure 4 depicts the processes of the proposed model for data protection in issuing graduation certificates.

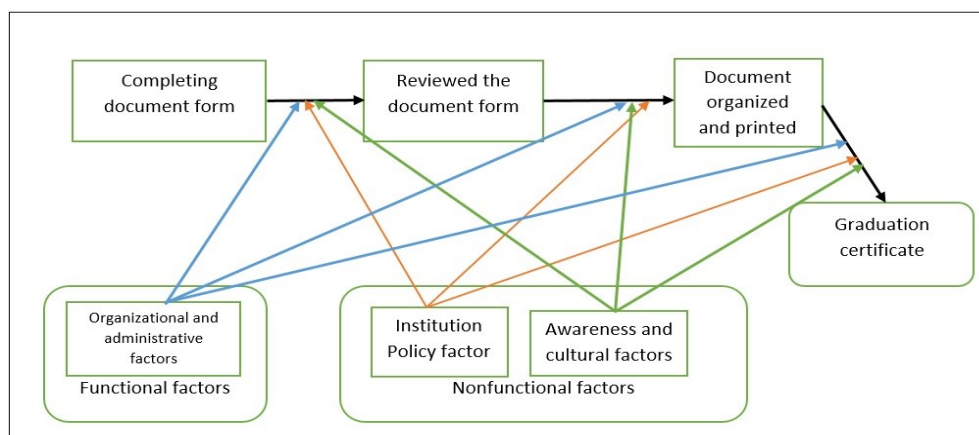


Figure 4. The proposed information system model with factors for issuing graduation certificate

4. COMPARISON OF RESULTS AND DISCUSSION

Previous research has focused on integrating security concerns, particularly access control mechanisms, during the final implementation stage. Others are more concerned with defining and analyzing security requirements. However, based on our review of previous research, we believe that no research has been done to effectively address the problem by identifying and specifying security demands and integrating them across the life cycle of a system. Research has resulted in a variety of methodologies, but they only cover a portion of the system's life cycle. Despite the importance of this aspect in the use and control of access methods in terms of safety, the requirements of any information system start from the organization's environment and objectives, and in most cases, the organizational aspects on which the information system operates are not taken into account. Based on these findings, we presented a model for delivering and evaluating security for all government departments and institutions. System administration, organizational factors, enterprise policy, awareness, and cultural features are among the most important security topics mentioned. Because it considers all functional and non-functional criteria, as well as social and organizational elements, the suggested model complements and enhances earlier models provided in the literature. Early in the requirements analysis process, safety features are addressed, and this consideration continues throughout the design process until implementation.

The proposed model is intended to protect information systems in government institutions in accordance with the institution's requirements, and the basic factors related to the organization and management are determined, as well as the basic responsibilities, which is important and necessary to protect information, as well as the definition of the institution's policy factors, particularly. Spreading awareness among the organization's employees is an important aspect of the proposed model, as it contributes to the protection of information and the systems that use it, as well as the development of the basic components of information systems represented by procedures related to technology and the institution's policy. These

procedures represent important steps to exploit time and determine priorities and roles that contribute to the implementation and protection of information systems and reduce the effort and time required to complete information security and protect the systems operating on it, as well as the speed of completion of system-related reports, which leads to improved management and security organs.

5. CONCLUSION

To successfully implement information system security using a variety of factors, apply these factors to the use of new information technology services, prepare a strategy and methods for implementing these factors with information technology services for each stage of the system, study and improve the institution's participation policy, and ensure its resiliency. To ensure the organization's good management, the security of the system and the user must be ensured. Because employees require security skills and knowledge of information technology, security measures are critical to ensuring that the system operates efficiently. In order to improve the security characteristics of information systems in government institutions, this research presented an information systems security model and, based on that, suggested the factors affecting information system security. The findings of this research will be useful in ensuring reliability and activating the use of electronic information systems. It will also be necessary to develop the methods of specialists who will be responsible for creating a comprehensive and efficient information system.

ACKNOWLEDGEMENTS

First, I would like to express our sincere gratitude to University of Baghdad for the continuous support of the research in our academic environment. Secondly many thanks to Universit Putra Malaysia (UPM) for all the knowledge we gain during our PhD and research journey.





REFERENCES

- [1] R. Gupta, S. K. Muttoo, and S. K. Pal, "Proposed framework for information systems security for e-governance in developing nations," in *ACM Int. Conf. Proceeding Ser.*, vol. Part F128003, pp. 546–547, Mar. 2017, doi: 10.1145/3047273.3047285.
- [2] M. Franeková, P. Holečko, E. Bubeníková, and A. Kanáliková, "Transport scenarios analysis within C2C communications focusing on security aspects," *ieeexplore.ieee.org*, 2018, doi: 10.1109/SAMI.2017.7880354.
- [3] D. W. Seo, W. S. Yi, and K. S. Lee, "Information security activities model per e-government service promotion stage," in *iiWAS2010 - 12th Int. Conf. Inf. Integr. Web-Based Appl. Serv.*, Nov. 2010, pp. 223–227, doi: 10.1145/1967486.1967523.
- [4] R. Villarroel, E. Fernández-Medina, and M. Piattini, "Secure information systems development—a survey and comparison," *Elsevier, Computers & Security*, Vol. 24, pp. 308–321. Jun. 2005, doi: 10.1016/j.cose.2004.09.011.
- [5] R. B. Vaughn, D. A. Dampier, and M. B. Warkentin, "Building an information security education program," *dl.acm.org*, Oct. 2004, pp. 41–45, doi: 10.1145/1059524.1059533.
- [6] R. M. Schneider, "A comparison of information security risk analysis in the context of e-government to criminological threat assessment techniques," in *Proc. 2010 Inf. Secur. Curric. Dev. Annu. Conf. InfoSecCD'10*, Oct. 2010, pp. 107–116, doi: 10.1145/1940941.1940966.
- [7] R. Ross, M. McEvilley, and J. C. Oren, "Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems," in *NIST Special Publication, National Institute of Standards and Technology*, 2016, 800-160, doi: 10.6028/NIST.SP.800-160v1.
- [8] R. Ross, P. Victoria, G. Richard, B. Deborah, and M. Rosalie, "Developing cyber resilient systems: a systems security engineering approach," 2019, No. NIST Special Publication (SP) 800-160, vol. 2 (Draft). National Institute of Standards and Technology, 2019, doi: <https://doi.org/10.6028/NIST.SP.800-160v2>.
- [9] Z. Soomro, M. Shah, J. A.-I. J. of Information, "Information security management needs more holistic approach: A literature review," *Elsevier*, vol. 36, pp. 215–225, 2016, doi: 10.1016/j.ijinfomgt.2015.11.009.
- [10] S. Flowerday, T. T. & security, "Information security policy development and implementation: The what, how and who," *Elsevier*, 2016, doi: 10.1016/j.cose.2016.06.002.
- [11] E. Niemimaa and M. Niemimaa, "Information systems security policy implementation in practice: from best practices to situated practices," *Springer, European journal of information systems*, vol. 26, pp. 1–20, Jan. 2017, doi: 10.1057/s41303-016-0025-y.
- [12] E. Crowley, "Information system security curricula development," in *Proc. 4th Conf. Inf. Technol. Curriculum, CITC4 2003*, Oct. 2003, pp. 249–255, doi: 10.1145/947121.947178.
- [13] D. Soares and F. De Sá-Soares, "Information systems security management key issues in local government," in *ACM Int. Conf. Proceeding Ser.*, Oct. 2014, pp. 227–230, doi: 10.1145/2691195.2691238.
- [14] H. Zafar, "Human resource information systems: Information security concerns for organizations," *Elsevier, Human Resource Management Review*, vol. 23, pp. 105–113, March, 2013, doi: 10.1016/j.hrmr.2012.06.010.
- [15] D. S. Bhilare, A. K. Ramani, and S. Tanwani, "Information security assurance for academic institutions using role based security metric: an incremental approach," in *Proc. Int. Conf. Adv. Comput. Commun. Control. ICAC3'09*, Jan. 2009, pp. 535–540, doi: 10.1145/1523103.1523209.
- [16] A. Asosheh, P. Hajinazari, and H. Khodkari, "A practical implementation of ISMS," in *7th International Conference on e-Commerce in Developing Countries: with focus on e-Security*, 2013, pp. 1–17, doi: 10.1109/ECDC.2013.6556730.
- [17] R. Baskerville, "Information systems security design methods: implications for information systems development," *ACM Comput. Surv.*, vol. 25, pp. 375–414, Jan. 1993, doi: 10.1145/162124.162127.
- [18] C. Sillaber and B. Ruth, "Using Business Process Model Awareness to improve Stakeholder Participation in Information Systems Security Risk Management Processes," *Citeseer*, In *Wirtschaftsinformatik*, pp. 1177–1190. 2015.
- [19] L. N. Amali, M. R. Katili, S. Suhada, and T. A. Labuga, "Business process monitoring system in supporting information





- technology governance," *beei.org*, vol. 10, no. 5, pp. 2884–2891, Oct. 2021, doi: 10.11591/eei.v10i5.3147.
- [20] A. Saleh, I.F.T. Alyaseen, "Successful factors determining the significant relationship between e-governance system and government operational excellence," *beei.org*, vol. 10, no. 6, pp. 3460–3470, Des. 2021, doi: 10.11591/eei.v10i6.2447.
- [21] A. Alkhuwaylidee, A. S. Almahdy, "Syrian E-Government Framework toward Government Excellence Servic." *Technologies for developing information systems TRIS-2019* (2019).
- [22] K. A. Barton, G. Tejay, M. Lane, and S. Terrell, "Information system security commitment: a study of external influences on senior management," *Elsevier, Computers & Security*, vol. 59, pp. 9-25, Jun. 2016, doi: 10.1016/j.cose.2016.02.007.
- [23] I. Arsad, D. Setyohadi, P. Mudjihartono, "E-commerce online review for detecting influencing factors users perception," *beei.org*, vol. 10, no. 6, pp. 3156–3166, Des. 2021, doi: 10.11591/eei.v10i6.3182.
- [24] N. S. Safa, R. V. Solms, L. Fitcher, "Human aspects of information security in organisations," *Elsevier, Computer Fraud & Security*, Vol. 2016, no. 2 : pp. 15-18, Feb. 2016, doi: 10.1016/S1361-3723(16)30017-3.
- [25] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and information security awareness," *Elsevier, Computers in Human Behavior*, vol. 69, pp. 151-156, Apr. 2017, doi: 10.1016/j.chb.2016.11.065.
- [26] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks," *Elsevier, computers & security*, vol. 68, pp. 145-159, Jul. 2019. doi: 10.1016/j.cose.2017.04.009.

BIOGRAPHIES OF AUTHORS







Dr. Haifaa Jassim Muhasin     she holds her PhD in A Multi-level framework for efficient sensitive data transmission in cloud computing from Universiti Putra Malaysia (UPM) in Information Systems, Faculty of Computer Science and Information Technology, Malaysia. She holds her MSc. in Computer Science/Data Security from the department of Computer Science and Information Technology, University of Technology, Baghdad, Iraq. She holds BSc. in Computer Science from the Faculty of Science, University of Baghdad, Iraq. Her current research interests are in data security, information systems, and cloud computing security. She is currently work as a senior lecturer in department of computer science, Faculty of Education for Pure Science (Ibn-Al-Haitham), University of Baghdad, Iraq. She can be contacted at email: haifajassim@yahoo.com and Haifaa.j@ihcoedu.uobaghdad.edu.iq



Ali Yahya Ghani     he holds his PhD from Universiti Putra Malaysia (UPM) in Information Systems, Faculty of Computer Science and Information Technology, Department of Software Engineering and Information Systems, Malaysia. He holds his MSc. from University College of Technology and Innovation (UCTI) in Information Technology Management, Department of Information Technology Management, Malaysia. He holds his BSc. in Computer Science from University of Baghdad, Department of Computer Science, Iraq. He is currently worked as a senior lecturer in University of Baghdad, Department of Co. Science. His research interest includes information systems, information technology management and software engineering. He can be contacted at email: ali.y.g@ihcoedu.uobaghdad.edu.iq



Hiba Adil Youisif     holds her MSc. from Universiti Putra Malaysia (UPM) in Software Engineering, Faculty of Computer Science and Information Technology, Department of Software Engineering and Information Systems, Malaysia. She holds his BSc. in Computer Science from University of Baghdad, Department of Computer Science, Iraq. She is currently work as a lecturer in University of Baghdad, Department of Co. Science. Her research interest includes software engineering and information systems. She can be contacted at email: hiba.a.y@ihcoedu.uobaghdad.edu.iq