Similarity and Dissimilarity between Information Security and Information Assurance

Nathaporn Utakrit* and Nattavee Utakrit**

Received : November 13, 2021
Revised : December 17, 2021
Accepted : December 21, 2021

Abstract

The advent of the Internet completely upends the globe and, in just decades, have changed everything about how people communicate and share and exchange information by establishing and maintaining the trust of the sources and staying secure. Safeguarding and protecting information is necessary. This article presents the understanding of information assurance (IA) versus information security (InfoSec) concepts. The paper aims to clarify the meaning, elements, and dimensions of IA and InfoSec and the relationship between the disciplines. Clarity of the dimensions and purposes of IA and InfoSec is important because this understanding serves as a foundation for the definition of curricula for the IA and InfoSec study program, responsibilities of IA and InfoSec practitioners, and corporate strategy and policy. The authors aim to present the measurements of the terms. The proactive and relevant official standards will also be introduced in the paper.

Keywords: information assurance, information security, confidentiality, integrity, availability, authentication, non-repudiation.

1. Introduction

In the modern era, information is increasingly a crown jewel. Data analytics reflects the importance of transforming raw and unstructured data into structurally processed data that becomes the Information of an organization or the vital corporate assets. Information, therefore, can gain valuable revenue to the organization if it has been utilized and stored properly. Some of the great potential in assurance and security of information are just that. In contrast, abuse or unawareness of information privilege as well as unauthorized access can cause troubles. Fraudulent activities on the Internet are mounting, resulting in infringement of the right to privacy as a crime. Beyond that, consumer frauds can result in financial loss and online transaction disruption. Protecting and securing such information are necessary.

The rapid advancement of Information and Communication Technology (ICT) and its infrastructure continuously intensify the interest in configuration hardening. Organizations pay increasing attention to information protection and security because the impact of information disclosure today has a more tangible, often devastating effect on business. Due to security concerns, corporations need to be unstoppable guard against information threats and hazards. Assets include but are not limited to patient information, bank client information, student information, and employee information.

Best practices for information require theoretical principles and application deployments. There are theories that relate to protecting and securing information. An information intensive environment, and security professionals have expanded the scope and thus the understanding of information and systems protection under an umbrella term referred to as information assurance [1]. Information security theory is related to the theory of information warfare as well as the theory of protection motivation [2]. Application deployment, also known as software deployment, usually involves installing, configuring, and enabling a specific application or set of applications, through an application manager or software management system, to a specific URL on a server [3].

Despite the fact that both information assurance (IA) and

* *Department of Information Technology, Faculty of Information Technology and Digital Innovation, King Mongkut's University of Technology North Bangkok.*
** *Department Information Technology Management, Faculty of Information Technology and Digital Innovation, King Mongkut's University of Technology North Bangkok.*

information security (InfoSec) have been defined elsewhere in the past, they are still vague in implementation and practice. The relationship between the two terms remains disputable. The study of Cherdantseva and Hilton [4] analyzed the ground theory of English literature in terms of goals associated with IA versus InfoSec based on the word origins and several authors' definitions from academies and industries. The implementation of these terms was not mentioned. Maconachy et al. [5] extended the InfoSec cube of John McCumber by addressing the authentication and non-repudiation becoming an IA model, and generally explaining model attribute definitions. Further, the authors introduced time which is the fourth dimension of the cube. Risk or exposure can occur at any given time during data access either on-line or offline and in the state of information and the information system is in flux.

Thus, the motivation of this article is to showcase the measurement in which these two terms have been mentioned. This article also originates from the necessity to resolve the overlap within IA and InfoSec concerning the overall scopes and dimensions of the disciplines. This paper analyzes different approaches to IA and InfoSec in order to draw a state-of-the-art picture of the disciplines in the changing landscape. The main objectives of this review are, firstly, to outline the up-to-date and precise realms of IA and InfoSec. Secondly, to develop an adapted refined definition of each discipline in light of these cases. The clarity and unambiguity of the scope and goals of an InfoSec are important because this knowledge serves further education, career objectives, and corporate missions and strategic policies.

2. Terms and Definitions

IA and InfoSec involve many related terms which can be dissimilar and partly overlapped. The National Security Telecommunications and Information Systems Security Committee (NSTISSC) and the Committee on National Security Systems (CNSS) defines information assurance as follows:

> *"Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and response capabilities"* [1].

The Free dictionary by Farlex website defined IA as follows:

> *"Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities"* [6].

Oxford dictionary defined information security as follows:

> *"Ways of protecting information, especially electronic data, from being used or seen without permission"* [7].

In addition, Cisco, also defined as information security, refers to the following statement:

> *"The processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection"* [8].

This section explains the definitions from the agents where both terms have been mentioned, as shown in Table 1. The bold fonts in the table emphasize the key meaningful terms. It can be seen that these agents have defined similar concepts of the IA and InfoSec. In brief, IA is the business practice of protecting information systems or organizations against overall risk. Whilst, InfoSec is the processes and methodologies implemented to secure information from any violation and failures. However, these two terms can still be entirely subjective from the definitions; the principle of these two terms can be explained for further distinction.

Table 1. *Linguistic levels classified by linguists.*

Sources	Information Assurance (IA)	Information Security (IS)
ICT Reverse	Information assurance is concerned with **all the overall risk and mitigations of an organization** [9].	The consideration of **technologies and software to be applied for keeping company operations safe and secure,** and enacting the strategies for infrastructure that are agreed during the information assurance process [9]
IGI Global	A **process centric phenomenon** that is comprehensive enough to include definition, implementation, and verification level operations [10].	The **securing of information** identified as confidential by computer-based and human-based procedures. [11]
PCMag Digital Group	The **technical and managerial measures** designed to ensure the confidentiality, possession or control, integrity, authenticity, availability and utility of information and information systems.[12]	The **protection of data** against unauthorized access.[13]
National Institute of Standards and Technology (NIST)	The **measures that protect and defend information and information systems** by ensuring their availability, integrity, authentication, confidentiality, and non- repudiation [14].	The **protection of information and information systems** from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability [15].
	Security assurance is the grounds for confidence that **the set of intended security controls or privacy controls in an information system or organization** are effective in their application [16].	Security information is **information within the system that can potentially impact the operation of security functions or the provision of security services** in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data [17].

3. Disciplines of Information Assurance and Information Security.

Despite the defined meanings, they still have overlapping concepts. Disciplinary paradigm is a common way to narrow down the IA and InfoSec realms with appropriate measurement theory in actions.

Figure 1. *CIA Triad.*

As shown in Figure 1, the CIA Triad is a benchmark model in InfoSec designed to be used in an organization while handling it in different approaches, such as stored, transmitted, or processed. Each attribute of the triad represents a critical component. CIA abbreviation comes from confidentiality, integrity, and availability. The meanings are explained as follows [18], [19], [20]:

- Confidentiality: Information is stored secretly. Only authorized users can access their private and sensitive information, such as date of birth, national id number, social security number, and tax information.
- Integrity: Information is displayed accurately and not tampered with in any way. An authorized person can only modify information.
- Availability: Information is promptly made available for the authorized person, excluding the scheduled maintenance, which is usually informed to the customers in advance.

Meanwhile, InfoSec is just a subset of IA. IA contains all the elements of InfoSec. Two additional elements under IA are authentication and non-repudiation, as shown in Figure 2.

- Authentication: The verification control needs to be put in place to ensure actual user authentication. In this regard, users must provide evidence of their identity prior to requesting any access to their confidential information.
- Non-repudiation: Both the sender and the recipient

Figure 2. *CIAAN Pentagon.*

of information are provided with proof of delivery and the proof of the sender's identity, so neither can later deny having processed the information [21]. Non-repudiation presents a proof of assurance to any activity in the system. Any activity for the user needs to be recorded and as evidence whether the action is successful or not.

Importantly, these two extra concepts underline IA. IA and InfoSec remain open to diverse interpretations, partly due to the fact that both disciplines are inevitably evolving in the corporate's strategy and practitioner experience. Although the elements overlap, the approaches to IA and InfoSec may vary. It depends on the background of an interpreter and practitioner [4].

4. Information Assurance and Information Security Official Document Coverages

IA encompasses logical protections and physical techniques. It is a superset of InfoSec and is the business outcome of information risk management. IA and InfoSec have been compiled into several standards and practices. The ISO/IEC 27000-series is known as the ISO27K. It is an international standard series published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This cooperation is a governance arrangement comprising the requirements of a structured suite of activities to manage information security risks. Information security risk management (ISRM) is an overarching framework through which management identifies, evaluates and addresses the organization's information risks. It ensures that the security arrangements and plans are fine-tuned with changes to the threats, vulnerabilities and business impacts. The standard covers all types of organizations, such as commercial enterprises, government agencies, nonprofits of all sizes, from micro-businesses to huge multinationals covering all industries. The industries include retail, banking, defense, healthcare, education and government [22].

Table 2 shows the ISO27K series related to IA and InfoSec. ISO/IEC 27001, launched in 2005, defines an Information Security Management System (ISMS) and complements the ISO/IEC 17799 code of practice standard in detailing several individual security controls. ISO/IEC 17799 was firstly published on a British Standard, namely BS 7799-1. ISO/IEC 27001 is also compatible with ISO/IEC 9001 quality management and ISO/IEC 14001

Table 2. *ISO 27K series related to InfoSec. [25]*

ISO-Norm	Title	Status
ISO 27000	Information security management system - Overviwe and vocabulary	Published 2009
ISO 27001	Information security management system - Requirements	Published 2005
ISO 27002	Code of practice for information securtiy management	Published 2007
ISO 27003	Information security management system implementation guidance	Published 2010
ISO 27004	Information security management - Measruement	Published 2009
ISO 27005	Information security risk management	Published 2011

environmental management. Later on, BS 7799-2:2002 was changed to ISO/IEC 27001 while ISO/IEC 17799 was changed to ISO/IEC 27002 in 2007 [23]. The international status of ISO/IEC 27001 will have a global impact on both information security management and certification. Organizations already certified under BS 7799-2:2002 need to prepare for the transition to ISO/IEC 27001 in order to meet its requirements [23]. The ISO/IEC 27001 is an audit standard based on verifiable requirements. The standard expresses the requirements for managing information security in organizations. The ISO/IEC 27002 is an implementation guideline based on best practice recommendations. The standard provides support and guidance for those responsible for implementing or maintaining an ISMS [24].

ISO 27000-27005 has been updated into several versions. ISO/IEC 27001:2013 determines the needs for establishing, implementing, maintaining and continually improving an ISMS within the organization's context. The standard includes generic requirements for the assessment and treatment of InfoSec risks tailored to the needs of the organization and intended to apply to all organizations, regardless of type, size or nature [26], [27]. ISO/IEC 27000:2018 specifies the overview of ISMS and terms and definitions commonly used in the ISO/IEC 27000 family of standards. It is designed to apply to all types and sizes of the organization, from multinational businesses to small and medium-sized enterprises (SMEs). The new version, which was released in February 2018, is equally valuable to government agencies or non-for-profit organizations. The recently published one provides an understanding of how the standards fit together: their terminology, scopes, roles, functions and relationship to each other [28], [29].

Although IA and InfoSec have their own pillars, there is no such distinguished name and scope when it comes to international standard recognition. IA and InfoSec have blended into an ISO27K family, which consists of several sub-standards. The standard established the approaches or methods to be used and identified relevant policies, such as the organization's risk tolerance or appetite. It also assesses qualitative and quantitative information risks, determines the likelihood of incidents, level of risk, and predicts the business consequences if they occur. Finally, the standard keeps stakeholders informed throughout the process and monitors and reviews risk treatments, any obligations and requirements on an ongoing basis, identifying and responding appropriately to significant changes [30].

5. Measurement theory in Action

IA and InfoSec professionals both seek the most secure physical data infrastructure to protect an organization’s information. Both terms leverage advanced technical safeguards, such as cutting-edge firewalls. An assessment of IA and InfoSec also illustrates an overlap in the threats they encounter. Both fields involve privacy issues and fraud, malicious hackers, and the strategic defense and retrieval of information systems prior to and post-catastrophic events. IA is a broader discipline that combines InfoSec with the business aspects of information management. IA typically involves implementing organization-wide standards to minimize the risk of threats harming a corporation. An IA team may overhaul login authentication systems or perform routine backups of critical organizational data to achieve this. Thus, IA professionals are more concerned with addressing the overall risk to an organization’s information than with individual threat. InfoSec, on the contrary, is a more hands-on discipline. It prioritizes developing tools, technologies, and other measures that can be used to protect the information from external threats. In academic perspective, the subtle distinction between the two fields may refer to earning a degree featuring both disciplines which can offer learners well-rounded skills and potentially support graduates to qualify for higher positions in the information security and assurance industries [31]. IA and InfoSec career paths for the graduates do not have a strict role. Each organization may classify the two fields as varied. WordWideLearn website [32]

lists out the jobs titles and responsibilities of IA that include computer security specialists, database administrators, computer and information research scientists, computer user support specialists, computer network architects, computer systems administrators, computer and information system managers, project managers, and local area network and wide area network managers. Moreover, Tripwire website [33] lists out the top 10 highest paying jobs in formation security that include chief information security officers (CISO), security directors, IT security architects, IT security managers, security engineers, malware analysts [34] penetration testers, IT security consultants, information security specialists, and forensic computer analysts.

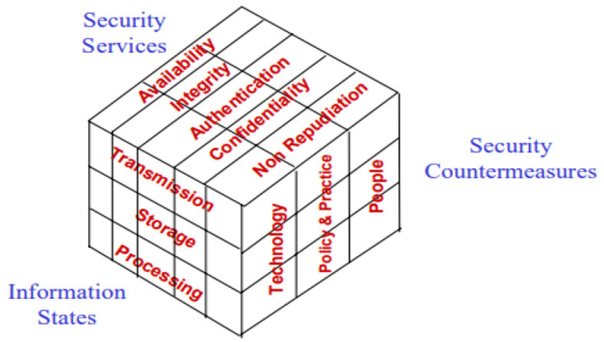

Figure 3. *Information Assurance Model extended from McCumber Cube [5].*

The McCumber Cube is one of the typical InfoSec schematics created by John McCumber in 1991. This security model depicts three-dimensional CIA triad critical information characteristics, Information states, and security measures. In developing IA systems, organizations must consider the interconnectedness of all the different factors that impact them [35]. The first dimension identifies the goals to protect information. These three principles aligned here are confidentiality, integrity, and availability. Maconachy et al. [5] modified the McCumber Cube model into an IA model that includes authentication and nonrepudiation, as shown in Figure 3. Confidentiality measures protect information against disclosure to parties other than the intended recipients. They are preserving authorized restrictions on information access and disclosure, including protecting personal privacy and proprietary information. Related questions would be: Is the data kept confidential? How is the data stored? Its security mechanism deals with hiding and covering of data which helps data become more confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into unreadable form without the right keys. It is achieved by two famous techniques named cryptography and encipherment. Level of data encryption is dependent on the algorithm used for encipherment. Whilst, integrity measures protect information or data being altered or destroyed by the attacker. Examples of system and information integrity controls include: flaw remediation, malicious code protection, security function verification, information input validation, non persistence, error handling, and memory protection [36]. The question would be: Does the selected approach help guarantee the integrity of data? This security mechanism is used by appending value to data. It is similar to sending a packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data is appended, checked, and is the same while sending and receiving data integrity is maintained. Finally, the availability measures ensure timely and reliable access to and use of information. The related question would be: Does the selected approach still make the data readily available to authorized users? Authentication assures the source of information to a receiving entity. Systems have a high order of availability to ensure that the system operates as expected when needed. Availability provides building of fault tolerance systems in the products. It also ensures the backup processing by including hot and cold sites in the disaster recovery planning. There are mainly two threats to availability of the system-denial of service and loss of data processing capabilities. Denial of service specifies actions that lock up computing services in a way that the authorized users are unable to use the system whenever needed, causing them to

be non responsive to the needs of users. The loss of data processing capabilities are generally caused by the natural disasters or human actions is perhaps more common. Contingency planning is the measure to counter such types of losses, which helps in minimizing the time that a data processing capability remains unavailable. Measurement implementation is multi-factor authentication in order for a user to reset a password using a combination of authentication which requires more than one form (e.g., text message to user, physical token). Security can enhance the access and flow of data and information by providing more accurate and reliable information and greater availability of systems. Access control is an example of authentication. Security mechanisms underneath can enhance individuals' privacy (e.g., encryption). Cryptography encodes the information with a defined algorithm known only to the originator and the recipient. Alternatively, steganography can be used to disguise the type of information by hiding a message in a bitmapped image [20]. However, some security mechanisms may present new vulnerabilities (e.g., single sign-on) [36]. That means once the attacker can gain access, it has the potential to get through all information at once within the system. Non-repudiation can ensure the authentication success or failure at each time that users access the system. It often involves the interchange of authentication information combined with provable time stamp access or log files. The second dimension of the security cube focuses on the problem of protecting the data in each of its possible states, including data in transit between information systems, storage (e.g., in memory or on a storage device), and process to achieve the desired objective. The third dimension defines the skills and disciplines the security professionals can call upon to protect information assets. Skills and knowledge in available technologies, devices, and products are essential to protect information systems and defend criminals. Security professionals are mastering the specialized software and hardware at their disposal. Notwithstanding, technological mastering is not enough to defeat criminals. Security professionals must also build a strong defense by establishing policies, procedures, and guidelines that enable users to stay safe and follow good practices. Finally, users must strive to become more knowledgeable about the online and offline threats and establish a culture of learning and awareness [31]. The professionals use a range of different skills and disciplines when protecting the data or information, being careful to always remain on the legitimacy.

Network security paradigms can also be classified amongst the scope of security measures taken (perimeter, layered), information states on how to carry information or data securely, and security services on how proactive the system is. In terms of information states, the use of intrusion detection systems (IDSs), which work to detect attempts to circumvent security measures, are required for modern business network environments for a high level of security. IDSs use various techniques to inspect intruders to penetrate a target system. It is deployed to ensure safe, and trust communication of information carried amongst organizations or individuals in all stages. The administrators can monitor the system of any attempt of security breach despite the success or failure of the attempts. Hence, alerting a network administrator to the potential for an attempted breach before the attempt is even initiated.

In a perimeter security countermeasure approach, the bulk of security efforts are focused on the network's perimeter. This focus covers firewall configuration, proxy servers, password policies, or any technology or procedure to make unauthorized network access less likely. Although the perimeter is secured, the various systems within that perimeter may show vulnerability. Other additional perimeter security includes physical security on fences, closed-circuit TV, guards, and locks, depending on the organization's security needs. Small organizations might use the perimeter approach that does not store sensitive data. They have budget constraints or inexperienced network administrators, although it is

clearly flawed and rarely works in a larger corporate setting. A layered security approach is one in which not only is the perimeter secured, but individual systems within the network are also secured. All servers, workstations, routers, and hubs within the network are secure. One way to accomplish this is to divide the network into segments and secure each segment as a separate network, so if the perimeter security is compromised, not all the internal systems are affected. This is the preferred method and should be used whenever possible [37].

IA and InfoSec practices can also support cloud computing. Apart from the customer's data, the issues of end-to-end security, privacy, and business integrity and continuity need to be more sophisticated concerns in cloud computing. In particular, cloud security, trust, multitenancy, encryption, and compliance are also in the coverage areas. Risk of security breaches and data leaks in business continuity and data-recovery issues, for the clients from sharing external resources, can cause loss of direct control of resources, increased liability, and reliability loss. Many cloud computing clients want to view access logs and audits trails of all users and vendors employees. The vendors should also assure data backup to an offsite location and maintain a resilient incident response model to ensure business continuity for the clients [38]. In addition, there is a high possibility of security threats in cloud IT infrastructures from storing critical and confidential data by the vendors. A survey by IT integrator Dataline of some 200 government officials in the US federal agencies reported that 64 percent of respondents had the topmost concern of adopting cloud computing security. However, obtaining accreditation for compliance with the Federal Information Security Management Act has shifted up the trust level towards cloud computing services acceptable for the public sector [39].

Further, mobile users who authenticate via their devices with confidential corporate information have increasingly been concerned about data security. InfoSec can focus on the confidentiality of information in transit and ensure the authorized partied access to information from different devices. In the InfoSec concept, developers need to ensure their IA applications do not compromise system security. The above mentioned concepts will eventually have a central role in shaping future IA applications and ensuring the manageable information achievement to the status of the legal records [20].

Furthermore, using professionals' investigative skills can find vulnerabilities before criminals exploit them. Professionals can plan ahead of a course of action to manage any associated risks. Their knowledge and intuitive experiences can alert them when and how risks may become problematic and determine the best way to limit the impact of a risk. Computer systems can be highly complex, but using related technologies can simplify the process by building a significant comfort level. As the fast growth of digital technology continues to evolve, professionals in IA and InfoSec need to extend their technological proficiency into quickly adapting to new tools and techniques as they are available in the industry. Teamwork and leadership skills are also a necessity when working in both fields. Facing a significant information security risk, one may need to rely on co-workers to eliminate the risk. Skilful leadership can unite team members to achieve remarkable goals.

6. Conclusions

InfoSec contains all the elements in IA. In other words, the elements of InfoSec all reside within the IA. Today, the distinct differences in IA versus InfoSec highlight the idea that the two fields deserve to be learned in independent subjects: IA is a manageable business approach which does not involve humans directly, and InfoSec is a practical approach which could happen to everybody who is unaware or is at risk. While IA focuses on the big business picture and seeks to know how a company uses information, how valuable it is to the company, and how exposed that information happens to be, InfoSec uses existing operating systems, applications, file systems, and hardware

platforms to house and secure information at rest and in transit, or create new systems, or new ways of combining existing ones and carries out the IA professional crafted and budgeted to protect organization's assets. That is why InfoSec is heard more often than the IA. However, working in both fields should not require the entire separation. IA and InfoSec should be parallelly applied into the organization's context appropriately, whether small, medium, or large organization. It depends on the job description and responsibility to secure individual information and corporate information as a whole from unwanted risks systematically.

7. References

[1] C.D. Schou, J. Frost, and W.V. Maconachy. "Information Assurance in Biomedical Informatics Systems." *IEEE Engineering in Medicine and Biology Magazine*,Vol. 23, No. 1, pp.110-118, January-February, 2004.

[2] C. A. Horne, S. B. Maynard, and A. Ahmad. "A Theory on Information Security: A Pilot Study." *Proceedings of the 14th Pre-ICIS Workshop on Information Security and Privacy*, Munich, pp. 1-23, 2019.

[3] Dialogic, *Application Deployment*. Available Online at https://www.dialogic.com/glossary/ application-deployment-, accessed on 17 October 2021.

[4] Y. Cherdantsevaa and J. Hilton, *Understanding Information Assurance and Security*, A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy, School of Computer Science & Informatics, Cardiff University, 2015.

[5] W. V. Maconachy, C. D. Schou, D. Ragsdale, and D. Welch, "A Model for Information Assurance: An Integrated Approach." *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy,* West Point, New York, pp. 306-310, 2001.

[6] The Free Dictionary, *Information Assurance*. Available Online at https://www.thefreedictionary.com/information+assurance, accessed on 29 October 2021.

[7] Oxford Learner's Dictionaries, *Information Security.* Available Online at https://www.oxfordlearnersdictionaries.com/definition/english/information-security, accessed on 29 October 2021.

[8] Cisco, *What is Information Security?* Available Online at https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html, accessed on 29 October 2021.

[9] Suzanne, *Information Assurance vs. Information Security.* Available Online at https://ictreverse.com/information-assurance-vs-information-security/, accessed 14 October 2021.

[10] IGI Global, *What is Information Assurance (IA).* Available Online at https://www.igi-global.com/dictionary/internal-auditing-information-assurance/14349, accessed on 17 October 2021.

[11] IGI Global, *What is Information Security (IS).* Available Online at https://www.igi-global.com/dictionary/information-security-is/14481, accessed on 17 October 2021.

[12] PCMag, *Information Assurance.* Available Online at https://www.pcmag.com/encyclopedia/term/information-assurance, accessed on 17 October 2021.

[13] PCMag, *Information Security*. Available Online at https://www.pcmag.com/encyclopedia/term / information-security, accessed on 17 October 2021.

[14] NIST, *Information Assurance (IA) - Glossary.* Available Online at https://csrc.nist.gov/glossary / term/information_assurance, accessed on 20 September 2021.

[15] Computer Security Resource Center (CSRC), *Information Security - Glossary.* Available Online at https://csrc.nist.gov/glossary/term/information_security, accessed on 20 September 2021.

[16] NIST, Security Assurance. Available Online at https://csrc.nist.gov/glossary/term/security_assurance, accessed on 20 September 2021.

[17] NIST, *Security Information - Glossary.* Available Online at https://csrc.nist.gov/ glossary/term/security_information, accessed on 20 September 2021.

[18] SentientDigitalInc, *5 Principles of Information Assurance.* Available Online at https://www.sdi.ai/blog/5-principles-of-information-assurance/, accessed on 14 October 2021.

[19] M. N. O. Sadiku, S. Alam, and S. M. Musa, " Information Assurance Benefits and Challenges: An Introduction." *Information & Security: An International Journal,* Vol. 36, pp. 3604-1-3604-5, 2017.

[20] R. Cummings, "The evolution of information assurance." *Computer*, Vol. 35, No. 12, pp. 65-72, 2002.

[21] Computer Security Resource Center (CSRC), *Non-repudiation - Glossary*. Available Online at https://csrc.nist.gov/glossary/term/non_repudiation#:~:text=Definition(s)%3A,deny%20having%20processed%20the%20information, accessed on 16 December 2021.

[22] *ISO27001Security, ISO/IEC 27001 certification standard*. Available Online at https://www.iso27001security.com/html/27001.html, accessed on 24 October 2021.

[23] The British Standards Institution, *ISO/IEC 27001 International Information Security Standard published.* Available Online at https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2005/11/ISOIEC-27001-International-Information-Security-Standard-published/, accessed on 2 November 2021.

[24] H. Baars, J. Hintzbergen, A. Smulders, and K. Hintzbergen, *Foundations of Information Security Based on ISO27001 and ISO27002 - 3rd revised edition. Zaltbommel*: Van Haren Publishing, 2015.

[25] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," *Journal of Information Security,* Vol. 4, No. 2, pp. 92–100, 2013.

[26] International Organization for Standardization, *ISO/IEC 27001:2013.* Available Online at https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54534.html, accessed 2 November 2021.

[27] M. Antunes, M. Maximiano, R. Gomes, and D. Pinto, "Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal," *Journal of Cybersecurity and Privacy,* Vol. 1, No. 2. pp. 219–238, 2021.

[28] International Organization for Standardization, *ISO/IEC 27000 – key International Standard for information security revised.* Available Online at https://www.iso.org/cms/render /live/en/sites/isoorg/contents/news/2018/03/Ref2266.html, accessed 2 November 2021.

[29] International Organization for Standardization, *ISO/IEC 27005:2018*. Available Online at https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/52/75281.html, accessed 2 November 2021.

[30] ISO27001Security, *ISO/IEC 27005 risk management standard.* Available Online at https://www.iso27001security.com/html/27005.html, accessed 2 November 2021.

[31] Norwich University Online, *Information Assurance vs. Information Security.* Available Online at https://online.norwich.edu/academic -programs/resources/information-assurance-versus-information-security, accessed 22 October 2021.

[32] WorldWideLearn, *Information Assurance Major.* Available Online at https://www.worldwidelearn.com/guide-to/technology/information-assurance-major/, accessed 16 December 2021.

[33] D. Bisson, *The Top 10 Highest Paying Jobs in Information Security – Part 2*. Available Online at https://www.tripwire.com/state-of-security/featured/

the-top-10-highest-paying-jobs-in-information-security-part-2/, accessed 16 December 2021.

[34] D. Bisson, *The Top 10 Highest Paying Jobs in Information Security – Part 1*. Available Online at https://www.tripwire.com/state-of-security/featured/the-top-10-highest-paying-jobs-in-information-security-part-1/, accessed 16 December 2021.

[35] J. McCumber, *Assessing and Managing Security Risk in IT Systems*: A Structured Methodology. Florida: CRC Press, 2004.

[36] M. Nieles, K. Dempsey and V. Y. Pillitteri, *An Introduction to Information Security.* Available Online at https://nvlpubs.nist.gov/nistpubs/ Special Publications/NIST.SP.800-12r1.pdf, accessed on 2 November 2021.

[37] C. Easttom, *Concepts and Approaches*. Available Online at https://www.pearsonitcertification.com/articles/ article.aspx?p=2990398&seqNum=6, accessed on 31 October 2021.

[38] R. Chakraborty, S. Ramireddy, T. S. Raghu and H. R. Rao, "The Information Assurance Practices of Cloud Computing Vendors," *IT Professional*, Vol. 12, No. 4, pp. 29-37, July-August 2010.

[39] E. Chabrow and R. Ross, *Rules Make Adoption of Cloud Computing Challenge for Agencies*. Available Online at https://www.govinfosecurity.com/rules-make-adoption-cloud-computing-challenge-for-agencies-a-1348, accessed 21 October 2021.