DOI:10.21276/sjeat.2017.2.3.3

Saudi Journal of Engineering and Technology **ISSN 2415-6272 (Print)**
Scholars Middle East Publishers **ISSN 2415-6264 (Online)**
Dubai, United Arab Emirates
Website: http://scholarsmepub.com/

Review Article

IT Security and Risk Management Certifications

Abdulhameed Jastaniyah[1]
[1]1609 Atlantic St-Bridgeport-CT-06604

***Corresponding Author:**
Abdulhameed Jastaniyah
Email: raze1212@hotmail.com

Abstract: The paper explores IT security and risk management certifications and compares them extensively to determine the best strategies for securing organization's information systems from unauthorized modifications and potential damages. It uses credible websites, such as ISACA and the International Information Systems Security Certification Consortium (ISC2) website to gather relevant information about their certifications. Furthermore, it relies on scholarly articles published by ISACA and ISC2 to obtain relevant information regarding cybersecurity and risk governance authorizations. With this strategy, the document evaluates each certification while listing their respective security domains and prerequisites. In using both the ISACA and ISC2 accreditation realms, the paper correlates the leading certifications offered by these associations. It also assesses the data results presented by these IT security institutions to determine their value to the information system maintenance and safety. Importantly, the document explains notable security strategies and controls that are listed in both ISACA and ISC2 credentials. With these approaches, the paper provides ideal security measures and procedures that are in line with specific accreditation to ensure a comprehensive safety computer system and asset protection. Subsequently, it explains important recommendations for effective information system support and operations resulting from ISACA and ISC2 accreditations domains.

Keywords: ISACA, ISC2, Certification, Information system, Cybersecurity, Unauthorized IT Security and Risk Management Certifications.

INTRODUCTION

Information is a significant asset in the modern technological environment. In fact, many companies become more reliant on their information systems, such as management information systems, transaction processing systems, and decision support systems, to conduct their daily operations [1]. Therefore, organizations are highly concerned about the proper use of such information, especially critical data. Importantly, the application of effective security controls on such business information systems preserves data integrity. This safety mechanism ensures that data remains original and it is not modified by an unauthorized party. Furthermore, strong data security restrictions guarantee information confidentiality in secure organizations. Such a strategy ensures that only authorized employees can access this data because it uses secure encryption procedures. Secure data also becomes available to the organization' staff when they need them. With availability, businesses experience continuity in times of emergency and data breach because it provides a safe mechanism of data backup and recovery plan [2]. In fact, in the event of information system attack, this availability offers the ideal solution since security engineers will block the access to the classified data while allowing the authorized user to view it. Therefore, the connection between confidentiality, integrity and availability plays a crucial role in establishing safe data that is used in a company's information systems.

The application of risk management certifications such as Certified Information System Audit (CISA) in an organization not only enhances the level of information security but also makes it effective for companies to acknowledge which security mechanism should be implemented in which structure (ISACA, n.d.). Such certifications ensure that the entire company's information has passed through various critical processes, including risk analysis, risk mitigation, and assessment. With risk analysis, the firm detects and analyzes dangers and the impacts of such threats on the available information. The strategy enables the managing staff to devise suitable recommendations of risk-mitigation measures. Risk reduction allows the organization to estimate,

implement, and keep the relevant danger-reducing controls that are favored for risk analysis. Therefore, risk management and IT certifications allow business enterprises to consider the requirements for developing, implementing, sustaining, and evaluating information security management systems to prevent unauthorized data alterations. The current paper discusses IT security and risk management certifications and compares them comprehensively to safeguard information systems and enterprise's assets from an unauthorized change and damage.

DISCUSSION

ISACA IT Security Certifications

ISACA provides significant certifications in the IT security field to affirm that the candidate is credible for analyzing the security level of a computer system. These certifications cover key areas such as information system auditing, safety management as well as IT governance and vulnerabilities. In line with IT security, ISACA (n.d.) provides the certified information system auditor (CISA) credential that authorizes professional informational system auditors. It guarantees that such information system inspectors have the necessary skills and competence to assess a specific computer system that operates in an organization. Furthermore, it ensures that certificate holders can manage the risks associated with such systems. For instance, a person can effectively institute protective strategies to prevent unauthorized personnel from accessing and interrupting a computer system [3]. Thus, certification grants the auditor a permit to inspect and analyze compliance at the organizational level. Predominantly, it allows this person to be accountable for all internal procedures and risks of an enterprise' technology network. Simply, it encompasses determining potential vulnerabilities in the information systems network and developing an action plan to avoid security infringement in such systems. What is more, the IT auditor can participate in preparing and implementing internal assessments procedures and developing internal audit reports. An interview conducted with Martin Zinaich, a CISA practitioner, reveals that the use of good IT governance is the best strategy to counter internal threats in an enterprise [17]. The auditor should also work within a cross-team to establish a stringent computer system infrastructure and cooperate with personnel to authorize and apply relevant policies and procedures concerning network security dilemmas [4]. Thus, the CISA credential investigates the competence to review enterprise information systems, risk management, and implementation of security controls of such systems.

Another key IT security certification is the certified information security manager (CISM) who covers domains of a secure cyberspace to prevent damages of computer systems at the enterprise level [15]. The CISM certification entails security governance, risk control, safety program development, and incidence response. Most importantly, the security governance domain covers all procedures that are related to maintenance, defining, and managing the security attempts of an enterprise. For instance, an ideal purpose of organizational governance is to make sure that the business will continue to exist and progress with time. Therefore, the common intention of security governance is to maintain business operations while seeking development and continuity [5]. Security governance should not only be seen as an IT problem but also as an issue that can affect the entire organizational process. According to Brandt [6], the implementation of security awareness program is significant for enterprises to stay secure because it educates the personnel on the potential threats and helps them maintain the organization's IT security policy. With this CISM certification approach, security management must address all aspects of a business enterprise such as acquisitions and mergers, divestitures and governance workforce. Thus, valuable organizational information and resources will be safeguarded from any form of unauthorized intrusion. Consequently, the CISM credentials analyze computer safety governance, risk management, security program development, and dangers response.

CISM credential also demands complete data integrity when assessing security governance and using risk procedures in managing information systems [15]. Integrity ensures that such computer systems are secured from data corruption and the interruption of services. Importantly, the basis of integrity assures that information is accurately maintained and kept consistent unless changes are made by the legitimate users. Since it is highly likely for the stored data to change due to careless access, the data integrity mechanism provides stringent measures to restrict unauthorized parties from modifying available data for personal use [2]. Therefore, the CISM accreditation requires the manager to ensure that the existing information security procedures can track and monitor authorized data usage and information distribution across a protected network.

Certified in risk and computer system control (CRISC) is the other fundamental IT security certification. CRISC authorization investigates the IT prowess and organizational risk management [15]. Substantially, with an efficient risk management procedure, the management at all levels of the enterprise will have access to all information they require to execute smart and sound decisions regarding which computer vulnerabilities to reduce, prevent. and eliminate. In fact, the failure of risk management

process can cause the organization to misunderstand the real magnitude of the dangers they encounter, and thus, expose them to potential attacks. Thus, certification requires that an information system should adopt a defined risk policy and standards to determine those permissible to the system so that the management could prevent the illegal access of data. With such standards, policies are defined on how they will be enforced in the information system. Identification and risk assessment procedures are also covered in CRISC certification. Such methods involve vulnerability scanning, program development analysis, regulation self-evaluation, and third-party program appraisal (ISACA, n.d.). Dangers prioritization and responsibility assignment are other risk management strategies that are covered in CRISC certification. With prioritization, risks are given various preferences, depending on the magnitude of the damage that such hazards cause to the information system. Responsibility assignment follows the prioritization procedures for controlling system risks. This is done by mitigating, avoiding, and accepting these dangers, especially where the worst may happen and the management is ready to live with the impacts [7]. Therefore, the CRISC accreditation evaluates cybersecurity and business risk management.

The certified in the governance of the enterprise (CGEIT) IT certification confirms the specialty in security principles and real ecosystem applications of IT governance (ISACA, n.d.). With IT management, business enterprise experiences effective administration of IT resources assisting it to attain specified goals. Predominantly, this IT security certification covers the complete governance of an institution but with a particular emphasis on enhancing the operation and management of information systems for the consequential gain of important stakeholders. Notably, the IT governance includes two major focus areas, such as demand governance and the supply-side management, that assist the management in formulating sound decisions for managing all IT infrastructures (ISACA, n.d.). The demand aspect of IT governance focuses on developing organization investment's decisions and technology inspection procedures that assist the business in maintaining all their computer systems safe. The demand side of IT governance also includes leading policies and principles, clear accountabilities, priorities, and benefit recognition of the entity's information system. Nonetheless, the supply-side management of IT governance puts greater emphasis on executing the IT operations and processes in the right way. Simply, computer system activities should be aligned with the existing policies and procedures to promote smooth business operation [8]. Therefore, with CGEIT IT security certification, the organization's IT infrastructure is guaranteed continuous transparency and accountability through the implementation of IT governance.

ISC2 Risk Management Certifications

The ISC2 institution plays a crucial role in managing enterprises' risks by providing security certifications that cover various areas, including security architecture, defense engineering, and safety control. Among the risks management certifications that it offers is the systems security certified practitioner (SSCP). This license is given to most security experts, involving network administrators, computer system inspectors, and security specialists that find it relevant to start their careers by acquiring the SSCP credentials (International Information Systems Security Certification Consortium Inc., n.d.). Such certification identifies security professionals, who are familiar with the major security principles, and those who can apply basic security mechanism to information systems in preventing unauthorized data modifications. It also distinguishes the system experts who can assess and apply countermeasures to bypass security hazards. The SSCP certification entails various domains such as access controls, security operations and management, risk identifications, audit and analysis, and danger response and recovery. Notably, Kelly [9] emphasizes that the use of proactive and reactive response controls, security monitoring, standardization, and assets recognition are the best IT security practices for organizations. Such risk management credentials also cover cryptography that is important to the information security of an enterprise by providing data encryption mechanism. The certification also encompasses network and communication safeguards as well as system and software security for a given entity. Therefore, SSCP authentication requires that an organization can utilize risk management procedures via analyzing potential dangers, considering the alternative approaches, and subsequently, implementing what the management opts to be the proper course of action.

Another key credential that focuses on risk management is the certified information systems security professional (CISSP). According to Gordon [10], the certificate distinguishes those IT experts who can construct, design, regulate, and manage the safety of an enterprise. Most predominantly, CISSP certification covers significant realm, including security and risk governance, asset safety, security architecture, and communication and network safeguards. It also includes the areas of computer maintenance and operations that involve information system control and activities external to the system that sustains its operation, for instance, keeping the documentation that provides useful guidelines on how to operate computer systems safely. Furthermore, CISSP credential considers software development protection strategies

that are essential in safeguarding the application running in computer systems. A good example is the software license management that ensures that the existing applications are well approved and the organizations take appropriate measures to guarantee that no illegal software is permitted in such systems. Cole [13] reveals other significant domains of CISSP accreditation such as cryptography, security model and plan, physical security and security governance strategies. Thus, CISSP authentication analyzes system development and design as well as cybersecurity control.

Certified authorization professional (CAP) accreditation recognizes the proprietors of enterprise systems and the security executives who approve and uphold information systems with a goal of balancing dangers with safety guidelines and countermeasures. Following these criteria, CAP certification is intended for the systems that are managed by private and public institutions such as the US government agencies like the State Department of Defense [14]. In fact, obtaining this important credential has significantly assisted the DOD staff to observe the 8570 decree (Department of Defense, n.d.). Thus, DOD is able to match the associated information risks with security specifications and employ corrective strategies to prevent its system from outside attack. Most importantly, CAP certification covers essential domains such as risk management framework, information system classification, security control strategies, implementation and assessment (International Information Systems Security Certification Consortium Inc., n.d.). Moreover, other areas that this risk control credential examines include computer system authorization and overseeing security restrictions of such a system. Subsequently, CAP credential assesses counter measures and security procedures used in enterprise systems.

The credential of certified secure software lifecycle professional (CSSLP) is provided to the software engineers who specialize in cyber security and application susceptibilities. The certification distinguishes expertise in web system security and software development life cycle (SDLC). Additionally, the accreditation approves the software experts who hold the proficiency of integrating safety procedures such as authentication, validation, and auditing into each stage of SDLC (International Information Systems Security Certification Consortium Inc., n.d.). Such security practices should be applied to a particular SDLC phase, from software creation and utilization to testing and launching. Because of these protection procedures, CSSLP authorizations have ascertained prowess in establishing an application security plan in running enterprises. They have also assisted in decreasing the system development costs, software vulnerabilities, and conveyance delays. Furthermore, organizations are become more credible in handling their data because safe and effective strategies are used to manage breaches, resulting from unsafe applications. Substantially, this certification covers essential domains, including software development principles, effective program specifications, reliable software development, and testing to develop web application systems that manage online risks (International Information Systems Security Certification Consortium Inc., n.d.). Thus, CSSLP authorization investigates web system safety and business SDLC.

The ISC2 offers certified cyber forensic professional (CCFP) accreditation to the experts who have a deep understanding of IT security, digital forensics, incidence reaction, and the legal ramifications of security investigation. Such IT professionals should also have the competence techniques that pertain mobile forensics, network forensics, electronic discovery, and other areas associated with risk management in cyber forensic. Furthermore, CCFP certification considers the proficiency in forensic techniques and operations, standards of procedures, and statutory and ethical codes to guarantee reliable, comprehensive, and authentic digital proof required in the court of law (International Information Systems Security Certification Consortium Inc., n.d.). It also recognizes the experts who are competent in using forensic data in other important domains such as malware assessment and incidence response procedures. Therefore, CCFP certification incorporates pertinent areas such as legal, moral principles, data analysis, forensic science, digital forensics, and risks related to the emerging technologies.

The healthcare information security and privacy practitioner (HCISPP) is another fundamental certification that investigates organizational risk management. This credential identifies computer experts who sustain the safety of healthcare information. With HCISPP, cybersecurity professionals will show competence in enforcing, regulating, and managing controls and countermeasure that safeguards therapeutic medical data and related digital files. Moreover, HCISPP authorization integrates various significant spheres such as healthcare entity risk control, environmental regulation, confidentiality and safety in health institutions and IT governance (International Information Systems Security Certification Consortium Inc., n.d.). It also covers healthcare systems risk management, information risks analysis, and third-party hazard management. Since HCISPP accreditation investigates critical therapeutic data, healthcare enterprises are required to ensure data confidentiality. With confidentiality, such information

is protected from illegal access because it maintains access control procedures that retain data protection. Thus, HCISPP accreditation investigates healthcare system risk management.

The Certified Cloud Security Professional (CCSP) accreditation is issued by both ISC2 and cloud security alliance to the experts who specializes in the safety of enterprise cloud computing and managing its related risks. According to Wu and Irwin [11], CCSP credentials recognize the persons who are competent in cloud technology so that they could make sure that the remote data is not only secure but also that security hazards and mitigation procedures are determined to resolve those risks. Furthermore, in his interview, Rattray reveals that utilizing cloud providers without safe IT infrastructure and service level agreement is the notable threat facing modern business agencies [12]. Principally, CCSP authentication involves essential domains that play a critical role in managing dangers associated with cloud computing security. These domains encompass cloud data safety, cloud implementation and infrastructure security, cloud operations, risk governance and the safety of cloud application (International Information Systems Security Certification Consortium Inc., n.d.). Hence, CCSP certification analyzes cloud computing security and risk governance.

Comparison of ISACA and ISC2 Risk Management Certifications

ISACA credentials investigate the enterprise computer systems, for instance, CISA accreditation that authenticates specialized information system auditors, and ISC2 credentials assess the use of safety principles and security strategies in such computer systems, for example, SSCP in comparison to ISACA credentials [15]. The CISA accreditation, which is offered by ISACA, ensures that IT inspectors have the necessary competence to inspect the security level of various information systems in an organization. It also guarantees that those, who are certified, can prevent and manage dangers related to such systems such as environmental, physical, technical, and site-support risks [6]. Furthermore, CISA authentication allows the auditor to evaluate and assess computer system compliance at the institutional level to determine if security controls are in line with safety standardization procedures. In comparison to ISACA certifications, ISC2 credentials, for instance, the SSCP certification, focus on the application of basic security concepts, security measures, system monitoring, and using effective countermeasures to avert potential security hazards. Consequently, SSCP accreditation assesses enterprise risk management strategies while CISA concentrates on information system safety review.

ISACA accreditations, for instance, CISM, deal with cybersecurity administration of an organization, while ISC2, for instance, CISSP, investigate risk governance, security maintenance, regulations, and software development safety strategies. Importantly, the CISM certification covers significant domains such as organization's security governance, cybersecurity risk management, secure software development procedures, and threats response (ISACA, n.d.). In contrast with ISACA credentials, ISC2, for instance, CISSP certification, allows an IT expert to develop, implement, and regulate the safety of an entity's information systems (International Information Systems Security Certification Consortium Inc., n.d.). Hence, ISC2 differs from ISACA, particularly CISM authentication because CISSP credentials focus on asset protection, security architecture, and data network security.

Another comparison between ISACA and ISC2 certification is that ISACA, for instance, CRISC accreditation, assesses company's risk management, while ISC2 credential, such as CAP investigates the credibility and security control procedures of an information system. At the same time, CRISC also concentrates on the appropriate policies and practices that a computer system should adopt to secure it from unauthorized access and interruption. It also maintains the identification and risk analysis procedures for safeguarding such systems (ISACA, n.d.). In contrast to such ISACA credentials, ISC2, mostly CAP certification, examines enterprise systems while concentrating on balancing system hazards with necessary security prerequisites and countermeasures. Another comparison of CAP to ISACA credentials is that it specifically reviews the management structure and the classification of cybersecurity systems to determine the appropriate strategies that the enterprise can use to safeguard its systems. Hence, CAP certification assesses the use of security procedures and authorization of information systems.

Furthermore, CGEIT accreditation, which is provided by ISACA, analyzes mainly business' IT governance, while ISC2, for instance, CSSLP, investigates web system security and SDLC (International Information Systems Security Certification Consortium Inc., n.d.). In fact, CGEIT authorization allows the management to effectively control IT applications to achieve its goals, and CSSLP certification incorporates web security procedures, including authentication, verification, and auditing a network application in comparison to CGEIT, an ISACA accreditation. Therefore, the concentration areas of CSSLP mostly include the use of stringent software concepts, reliable software requirements, safe program development, testing, approval, and

procurement, while the domain of CGEIT, an ISACA certification, is IT governance.

An Interview with Mr. Gregg Bjork

Can you please provide your experience in the field of information security?

He said he has been involved in developing technologies for the past 30 years. All of the products that I participated in had an element of security whether that was access control, auditing, governance, or full data security. He has done this commercially for information security for enterprises, as well as for consumers.

What are the information security and risk management certifications that you recommend students to take to get a good job in that field?

There are many good certifications that could prove valuable to anyone who wishes to make a living in the security field. It depends on what your focus area will be (i.e., hacking, operations, access, etc). I highly recommend the certifications provided by [16]2 (https://isc2.org/credentials/default.aspx). If someone completes these certifications, they will be well equipped to start a career in information security.

What kinds of experience outside of the classroom are helpful in cultivating expertise in the field?

The most useful real world experience comes from working with a security company, or a technology company with security has a main component of their offerings. Self-taught, self-paced learning is always encouraged. There is nothing that replaces experience in this domain.

CONCLUSION AND RECOMMENDATIONS

Cybersecurity is essential to modern business enterprises because it ensures that information systems, data, and application programs are safeguarded from unauthorized access, modifications, and intrusion. In guaranteeing stringent security to such systems, organizations use effective security policies and controls to maintain data integrity. Furthermore, these institutions ensure that their computer systems are integrated with strong data security controls to uphold information confidentiality. They also make sure that the information in the system is available to the authentic parties, and data backup and recovery procedures are functional. Therefore, data integrity, confidentiality, and availability are important because they guarantee that organization's data is safe from unauthorized use. Predominantly, the utilization of risk management credentials from both ISACA and ISC2 makes them useful for institutions to determine effective defense strategies that are applicable to their computer systems. ISACA provides necessary accreditations, including CISA, CISM, CRISC, and CGEIT that are ideal for analyzing enterprise IT security. Contrastingly, ISC2 offers relevant certifications, such as SSCP, CISSP, CAP, CSSLP, HCISSP and CCSP, that crucial for securing organization's assets.

Organization's management should ensure that such credentials are utilized to enhance all levels of organization's IT security and risk governance. In line with this strategy, necessary procedures should be adopted in computer system support and operations. Such procedures should cover user support to enhance information security. Collectively, the system support and operations document should offer guidance to computer users by creating awareness through detecting and managing possible security threats. Proper regulations should also be integrated into the organization's information system software that is consistent with the potential risks. Furthermore, such regulations should contain policies for installing and starting new applications on a computer system to prevent bugs. Proper configuration management and media controls must also be applied to computer systems to prevent any form of data intrusion. Configuration controls should also guarantee that modifications on such system do not involuntarily interfere with data security. Additionally, system defenses must be filed, including safety procedures, contingency controls, and security policies and practices. Such practices should also be maintained to guarantee that only authorized parties can access the system. Hopefully, the application of ISACA and ISC2 accreditations, as well as these recommendations, will protect organization's systems, application programs and all valuable assets from unauthorized activities.

REFERENCES

1. Whitman, M. E., & Mattord, H. J. (2013). Management of information security (4th ed.). Boston, MA: Cengage Learning.
2. Stamp, M. (2011). Information security: Principles and practice (2nd ed.). Hoboken, NJ: Wiley.
3. Mattsson, T. (2014). Intersectionality as a useful tool: Anti-oppressive social work and critical reflection. Affilia, 29(1), 8-17.
4. Ross, S. J. (2015). Information security matters: Are software flaws a security problem? ISACA Journal,
5. Stallings, W., & Brown, L. (2014). Computer security: Principles and practice (3d Ed.). Pearson, MA: Boston.
6. Aad, G., Abbott, B., Abdallah, J., Abdinov, O., Aben, R., Abolins, M., ... & Abulaiti, Y. (2016). Measurements of the Higgs boson production and decay rates and coupling

strengths using pp collision data at\ sqrt {s}= 7 and 8 TeV in the ATLAS experiment. *The European Physical Journal C*, *76*(1), 6.

7. Goodrich, M. T., & Tamassia, R. (2011). Introduction to computer security. Boston, MA: Pearson.
8. Sharkasi, O. Y., & CBCP, C. (2015). Addressing Cybersecurity Vulnerabilities.
9. Abbott, B. P., Abbott, R., Abbott, T. D., Abernathy, M. R., Acernese, F., Ackley, K., ... & Adya, V. B. (2016). Observation of gravitational waves from a binary black hole merger. *Physical review letters*, *116*(6), 061102.
10. Mardirossian, N., & Head-Gordon, M. (2014). ωB97X-V: A 10-parameter, range-separated hybrid, generalized gradient approximation density functional with nonlocal correlation, designed by a survival-of-the-fittest strategy. *Physical Chemistry Chemical Physics*, *16*(21), 9904-9924.
11. Wu, C. H. J., & Irwin, J. D. (2016). *Introduction to computer networks and cybersecurity*. CRC Press.
12. Infosec Professional. (2012). Interview series - Jo Stewart-Rattray VP of ISACA.
13. Cole, E. (n.d.). Leadership laboratory. Interview by S. Northcutt.
14. Department of Defense. (n.d.). Certifications: DoDD 8570. Retrieved from http://www.giac.org/certifications/dodd-8570
15. ISACA. (n.d.). ISACA certification: IT audit, security, governance and risk. Retrieved from http://www.isaca.org/CERTIFICATION/Pages/default.aspx
16. International Information Systems Security Certification Consortium Inc. (n.d.). (ISC) ² Information Security Certification Programs. Retrieved from https://www.isc2.org/credentials/default.aspx
17. Online Education. (n.d.). Interview with Martin Zinaich, Information Security Officer, city of Tampa. Retrieved from https://www.onlineeducation.com/expert-interviews/martin-zinaich-city-of-tampa