IMPACT OF ORGANIZATIONAL SECURITY CERTIFICATION ON OPERATIONAL SECURITY: EXAMINING THE RED TAPE

by

JESSICA BUTEL

M.S., Western Governors University, 2018

M.B.A., Western Governors University, 2021

A Research Paper Submitted to the School of Computing Faculty of
Middle Georgia State University in
Partial Fulfillment for the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA
2023

Impact of organizational security certification on operational security: Examining the red tape

Jessica Butel, *Middle Georgia State University, USA, jessica.butel@mga.edu*

Abstract

This thematic literature review examines the relationship between operational security and organization security compliance that is driven by a requirement to achieve a security certification or accreditation. The findings of this research seek to identify the themes associated with efforts to meet the requirements of industry certifications or accreditations on the state of operational security within an organization. Emerging themes were developed by grouping the identified contributions from the iterative analysis of key articles, then the themes were examined to develop a theoretical model. The model highlights the resource contention within the organization and the masking of practical security risks are two potential negative impacts security compliance can have on operational security.

Keywords: security certification, ISO 27001, security compliance, operational security, practical security

Introduction

News channels in the United States commonly report that cyber-attacks are increasing frequently. In the United States, the average cost of a data breach in 2022 was $9.44 million, demonstrating the significant losses organizations face during a compromising event (IBM, 2022). These costs may be associated with addressing damages directly related to the exposure of an individual's data that an organization had collected. The application of a security framework to an organization's cybersecurity program is assumed to ensure the protection of its information systems and data. Organizations and interested third parties may assume that adherence to a chosen security framework results in a secure operational environment, reduces the risk of security incidents, and ensures the protection of sensitive information. In 2018, Morrison and Kumar documented that executives expect future increases in cybersecurity regulatory scrutiny of 57.3% and demands for internal reporting on cybersecurity program effectiveness of 62.7% (Morrison & Kumar, 2018). Some industries are regulated and required to maintain industry accreditation, such as compliance with the Payment Card Industry (PCI) Data Security Standard (DSS), to process credit or debit card transactions (Razikin & Widodo, 2021). Organizations may also seek a security certification or accreditation to demonstrate the effectiveness of their security measures, gain customer trust, and showcase the security of their environments (Hampton et al., 2021). For example, organizations offering information technology products or services may consider an industry certification, such as ISO 27001, or an industry accreditation, such as System Organization Controls (SOC) for Service Organizations Type 2, to demonstrate the security of their systems or products.

Problem Statement

Security concerns plague organizations as they attempt to protect their customers' information and other sensitive data. To assure customers that the organization's systems are safe, the organization may leverage industry certifications or accreditations of its environment. However, the external assessor's evaluation of an organization's compliance with a security framework may not always translate to operational security. Therefore, it is imperative to understand how industry certifications or accreditations relate to an organization's operational security to recognize whether these attestations should be trusted as a demonstration of security.

Purpose of the Study

This study examines the relationship between operational security and security framework compliance that is driven by a requirement to achieve an industry certification or accreditation.

Research Question

Consistent with the purpose of this study, the following research question is asked:

RQ: What themes can be identified when organizations consider how compliance with a security framework, necessary to achieve an industry certification or accreditation, impacts operational security?

Research Objectives

The findings of this research will highlight emerging themes concerning the impact of striving to meet the requirements of industry certifications or accreditations may have on the state of operational security within an organization. These themes will be examined to develop a model to better understand the relationship between an organization's operational security and its state of compliance with a security framework.

Review of the Literature

Determining Operational Security

Within academic research focused on the information technology (IT) field, there are a plethora of definitions appropriate for cybersecurity. Operational or practical cybersecurity is generally defined as the implementation of technologies to ensure the confidentiality, integrity, and availability of an organization's information and infrastructure by researchers and IT professionals. To further refine the scope for the purposes of this research, it is necessary to focus on operational security. Operational security can be defined as the practical expression of an organization's security posture. Rather than the theory of information security, operational security is the acting state of an environment and encompasses the compromises in security design necessary to conduct the organization's business activities. When considering operational security, there are three types of security-related resources that can be described as information security technologies, qualified information security personnel, and organizational users' security awareness (Cavusoglu et al., 2015).

Defining Security Compliance

Security compliance is generally accepted as the measurement to which an organization adheres to a security framework such as NIST CSF or ISO/IEC 27001 (ISO 27001). Security frameworks provide guidance concerning policies, procedures, and processes designed to secure the confidentiality, integrity, and availability of IT environments. Frameworks can be used by organizations to structure their efforts to protect critical assets and information necessary for their business operations. ISO 27001, most recently updated in 2022, is a widely known standard focused on providing a framework describing an information security management system (ISO, 2022). The ISO 27001 standard is supported by other publications, such as the ISO 27002, that offer implementation or auditing guidance (ISO, 2022). An organization seeking ISO 27001 certification must engage with a third-party auditor who evaluates the organization's compliance with the appropriate standard or framework. As industry guidance advances, an identified shortfall of historical compliance measurements is the point-in-time nature of the assessments, which may not represent an organization's normal business practices (NIST, 2018). The assessors measuring compliance are transitioning the focus to a continuous monitoring assessment to better capture an organization's operational security (NIST, 2018).

Organizational Certification Purpose

The research covers many compliance frameworks, certifications, and accreditations, including but not limited to ISO 27001, NIST Risk Management Framework (RMF), PCI DSS, SOC 2, Committee on Foreign Investment in the United States (CFIUS) Foreign Investment Risk Review and Modernization Act of 2018 (FIRRMA), and Federal Risk and Authorization Management Program (FedRAMP). Organizations may pursue certification or accreditation for their environment as a requirement or as an optional endeavor. Some environments require certification in order to process certain data, such as PCI DSS to handle credit card transactions, or certification to be considered acceptable for use, such as FedRAMP for United States federal government entities. The United States Securities and Exchange Commission (SEC) imposes requirements, defined in the Sarbanes-Oxley (SOX) Act, through civil enforcement on publicly traded organizations. Organizations with substantial foreign interest or investment may be subject to Committee on Foreign Investment in the United States (CFIUS) requirements, including annual audits to avoid penalties from the United States government. Organizations can elect to undergo certifications without an enforced requirement, such as ISO 27001, to provide third-party assurance of their security program to external interested parties. Large organizations are unable to expose internal protection measures and security processes to the multitude of customers who may be interested due to concerns such as sharing sensitive business information or lack of available resources. Certifications, accreditations, or attestations may be provided to external entities as the assurance of the organization's product or environmental security. Organizations may seek certification or accreditation to demonstrate the compliance of their security to an industry security framework in an effort to gain customer trust (Hampton et al., 2021). In addition to ISO 27001, System and Organization Controls (SOC) 2, self-attestation to a NIST framework, or BSIMM might be considered by an organization as an optional method to measure the maturity of their information security program.

Operational Security Effectiveness

Existing literature has examined approaches to measuring operational security effectiveness. Reviewing this research provides insight into the measurement of security efficacy over time. In the current landscape, the cost and frequency of a data breach of an organization's information or systems are still on an upward trajectory (IBM, 2022). The effectiveness of an organization's information security program is determined by many complex facets and has proven challenging to accurately measure (Steinbart et al., 2016). Industry reports indicate that organizational security compromises could be prevented or identified earlier through the application of industry best security practices resulting in more effective operational security (Verizon, 2022). There are indications that demand for internal reporting from executives on cybersecurity program effectiveness will increase by 62.7%, highlighting the need to measure the implementation of efficiencies of operational security implementation (Morrison & Kumar, 2018). Published research describes challenges organizations face when attempting to capture a measurement for their operational security effectiveness.

To measure operational security effectively, an organization must have individuals who are sufficiently knowledgeable about the operational details of the organization and are willing to disclose weaknesses or deficits in the organization's security implementations (Steinbart et al., 2016). Previous research has developed a conceptual model relevant to security efficacy, but the proposed model does not provide an accurate measurement of effective operational security. Instead, the model captures the users' perception of security when the environment is compliant with a selected security framework (Kankanhalli et al., 2003). A more complex instrument, SECURQUAL, considers five dimensions, including successful and unsuccessful security exploitation events, which may be closer to measuring operational security efficiency in relation to compliance (Steinbart et al., 2016). As researchers work to comprehensively test SECURQUAL, questionnaires are used, which continues the challenge of trying to judge security effectiveness based on the responses of individuals without technical data (Prislan et al., 2020). Frameworks, such as MITRE ATT&CK, aim to categorically test the security of the layers of an environment through attempted technical exploitation (Strom et al., 2020). To understand the protection that framework compliance may provide, the MITRE ATT&CK framework has been tested against NIST SP 800-53 to demonstrate which security configurations would prevent an exploit from successfully running (Rahman & Williams, 2022).

Methodology

Procedure

Selected articles meeting defined inclusion criteria were reviewed with a narrative approach (Jones, 2004). Articles were found through a set search string of “security” AND (“efficiency” OR “effectiveness” OR “efficacy”) AND (“ISO” OR “NIST” OR “PCI” OR “FedRAMP” OR “SOC II”) in GALILEO, Google Scholar, and IACIS journals. Abstracts were reviewed for relevance to the topic of this research paper when the article met the eligibility requirements of this research. Eligibility requirements included the publication date within the last 20 years, the full text being available, and written in English. From the initially identified key articles, supplementary articles were found based on forward and backward citation searching and were included to gather an appropriately sized library (Webster & Watson, 2002). All supplementary articles had to meet the previously established eligibility criteria. To identify appropriate themes, the constant comparison method to develop a construct to document the analysis (Glaser & Strauss, 1967).

Analysis

An iterative analysis using the constant comparison method, as opposed to the analytic induction method, due to the focus on generating theory in this research, was employed (Glaser & Strauss, 1967). No a priori hypotheses were used to identify themes in this research. The articles meeting the inclusion criteria were used to conduct the narrative review. Emerging themes concerning the relationship between operational security and security framework compliance were developed by grouping the identified contributions from the iterative analysis. The emerging themes were examined to develop a theoretical model to better understand the relationship between an organization's operational security and its state of compliance with a security framework (Webster & Watson, 2002). Table 1 includes the key articles with the author(s) and titles selected for this research. Table 2 depicts the theme analysis consisting of the theme, authors(s), and theme ID.

Table 3: Key Articles

Author(s)	Title
Ojalainen, 2020	Iso 27001 Information Security Management Standard's Implementation in Software Development Environment: A Case Study
Siponen, 2006	Information security standards focus on the existence of the process, not its content
Zandona & Thompson, 2017	Going beyond Compliance: A Strategic Framework for Promoting Information Security in Hospitals
Hsu, Wang & Lu, 2016	The Impact of ISO 27001 Certification on Firm Performance
Fomins, de Vries & Barlette, 2008	ISO/IEC 27001 information system security management standard: exploring the reasons for law adaption
Breier, 2014	Security Evaluation Model based on the Score of Security Mechanisms
Sharma & Dash, 2012	Effectiveness of ISO 27001, as an information security management system: an analytical study of financial aspects
Andersson, Hedström & Karlsson, 2022	Standardizing information security–a structurational analysis
Beckers et al., 2014	A structured comparison of security standard
Slapničar et al., 2022	Effectiveness of cybersecurity audit

Table 2: Theme Analysis

Theme	Author(s)	Theme ID
Standard of work same as prior to ISO 27001	Ojalainen, 2020	2b
Processes perceived as slower, more rigid	Ojalainen, 2020	1d
Certification does not enforce technical implementation to operational security	Ojalainen, 2020	2a
No guidance on practical implementation creates conflict on how to meet the requirements of certifying standard	Ojalainen, 2020	1d
Meeting certification requirements is time-consuming, and less time for operational tasks	Ojalainen, 2020	1d
Certification requirements can create fear/apprehension about completing operational activities	Ojalainen, 2020	2d
Interpreting the standard requirements was found to be stressful and tiring	Ojalainen, 2020	1c
Lack of top-management support through the certification process felt by employees	Ojalainen, 2020	1c
Certification requirements focus on process existence, not content	Siponen, 2006	2a
Meeting certification requirements may provide a false sense of security	Siponen, 2006	2a
Accreditation costs to achieve security certification are high	Hsu, Wang & Lu, 2016	1b
Implementation costs to achieve security certification are high	Hsu, Wang & Lu, 2016	1b
Security certifications may not improve an organization's financial performance	Hsu, Wang & Lu, 2016	1b
High effort and time costs to reach organizational certification	Fomins, de Vries & Barlette, 2008	1d
The generality of certification guidelines does not match the specificity of business processes	Fomins, de Vries & Barlette, 2008	2a

Table 2: Theme Analysis (Cont.)

Theme	**Author(s)**	**Theme ID**
Adoption of the standard may require specialized experience	Fomins, de Vries & Barlette, 2008	1a
Standard only investigates the presence of the process, not the quality of the process	Breier, 2014	2a
ISO is not well-positioned to measure operational security without dependencies	Breier, 2014	2a
Possible to be compliant with ISO 27001 and insecure	Sharma & Dash, 2012	2a
Effective information security requires knowledgeable and qualified personnel	Sharma & Dash, 2012	1a
Effective information security requires management sponsorship	Sharma & Dash, 2012	1c
Effective information security requires user participation and support	Sharma & Dash, 2012	1c
Successful certification does not focus on how well security processes are followed	Sharma & Dash, 2012	2a
Security regulations challenge to measure operational security due to being broad and lacking sensitivity to the organization's industry	Andersson, Hedström & Karlsson, 2022	2a
Security regulations challenge to measure operational security due to a lack of focus on the content of a process	Andersson, Hedström & Karlsson, 2022	2a
Even when a cybersecurity audit is considered effective, the organization is still vulnerable	Slapničar et al., 2022	2a
Limited organizational resources can impact audit frequency and timelines	Slapničar et al., 2022	1b
Limited organizational resources can delay or prevent remediation actions.	Slapničar et al., 2022	2b
Cybersecurity audit engagements are most effective when receiving sufficient resources	Slapničar et al., 2022	1b
Security standards are complex and time-consuming for technical staff to understand	Beckers et al., 2014	1d
Demonstrating adherence to security controls can require interpretation and be ambiguous	Beckers et al., 2014	2a
A plethora of security standards published results leaves challenges in measuring security controls meaningfully	Beckers et al., 2014	2a
No framework covers how to incorporate security features into security technologies	Poehlmann, et al., 2021	2a
Translating security controls takes significant time	Poehlmann, et al., 2021	1d

Results

The implementation of compliance controls does not guarantee that the controls are capable of accurately measuring the effective security posture of an environment. The numerous security standards published pose challenges in terms of interpretation, application, and meaningful measurement of recommended security controls (Beckers et al., 2014). Moreover, the introduction of additional requirements creates more work for technical resources, leading to conflicting views within an organization on how duties should be prioritized. Prioritizing compliance activities for technical resources may be difficult for them to comprehend, as some individuals believe that the implementation of ISO 27001 certification would not raise their current standard of work (Ojalainen, 2020).

Capturing an organization's compliance with security regulations presents further challenges in accurately measuring operational security. Arguments against the ability of security regulations to accurately capture the efficacy of operational security include their broadness, lack of tailoring to the industry, lack of focus on process content, and failure to measure essential components due to narrow scope of review (Andersson et al., 2022). Furthermore, additional complexity could be added to the discussion of compliance as other research focuses on understanding the effectiveness of cybersecurity audits on security risk management (Slapničar et al., 2022). The proposed model has been developed by summarizing these themes from key research articles to gain a better understanding of the potential impact that compliance can have on operational security.

Whether compliance activities are driven by optional or required certification efforts, this research has not uncovered a notable difference in the frequency or magnitude of potential negative impacts mentioned in the reviewed articles. The major themes fall into two significant impact categories: (1) resource contention within the organization, and (2) masking of practical security risks. Within the category of resource contention, the identified factors include (1a) qualified advisors, (1b) financial considerations, (1c) employee interest, and (1d) work effort. Within the category of masking practical security risks, the identified factors include (2a) compliance with the standard does not guarantee security, and (2b) employees may fear identifying gaps in operational security as they appear due to uncertainty surrounding the compliance standard or concern for disrupting the certification efforts.

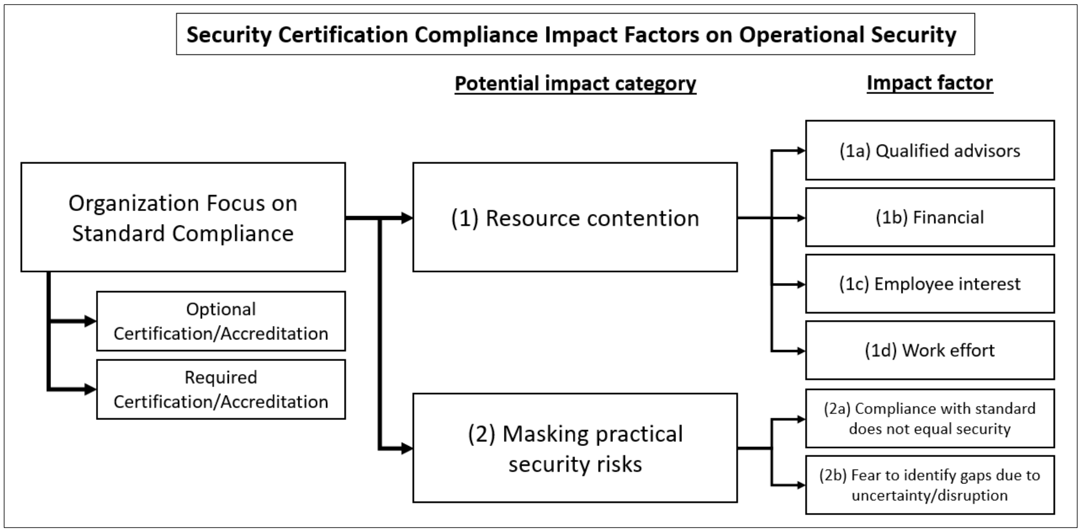
Security Certification Compliance Impact Factors on Operational Security
Potential impact category
Impact factor
Organization Focus on Standard Compliance
Optional Certification/Accreditation
Required Certification/Accreditation
(1) Resource contention
(2) Masking practical security risks
(1a) Qualified advisors
(1b) Financial
(1c) Employee interest
(1d) Work effort
(2a) Compliance with standard does not equal security
(2b) Fear to identify gaps due to uncertainty/disruption

Figure 1: Potential Impact Categories and Factors

Discussion of Findings

Compliance with security standards is often seen as necessary for achieving organizational security certification or accreditation, regardless of whether it is optional or required. Research and industry trends suggest that compliance efforts can provide direction, structure, and benefits to an organization's security posture (Vance, et al., 2012). However, without a method to measure the efficacy of operational security and compliance coverage, the understanding of the impact of framework compliance on operational security may be incomplete. This literature review focuses on identifying themes that highlight the potential negative impacts of compliance on operational security. The emerging themes suggest that not all impacts of compliance are beneficial for practical security. This relationship may be further complicated by the challenges in measuring operational security efficacy. It can be argued that if security controls' effectiveness in an organization's information technology infrastructure is difficult to measure, then a certification designed to enhance security through adherence to security standards may be lacking in necessary components for success.

Implications of Findings

These findings imply that organizations need to be aware of the potential negative impacts of certification or accreditation efforts on their operational security when considering their goals. In research, compliance with security standards is often discussed only in terms of positive impacts on an organization's security environment. When creating a roadmap towards organizational security certification, it is important to consider potential pitfalls so that organizations can better prepare and monitor their operational security posture for impacts from certification efforts. Organizational resources are finite and must be intentionally allocated to best serve the organization's business. An accurate evaluation and understanding of how certification efforts can create resource contention with operational security is crucial for organizations to grasp. Additionally, individuals who view certification reports as conclusive evidence of the security of an information technology environment must be mindful that operational security may be masked by organizational security certification. The findings indicate that documenting compliance with a given security standard does not necessarily mean that the processes identified as meeting the security controls are evaluated for their effectiveness. Security controls are not always an accurate measure of how effective an environment's security is. This model, along with the findings, serves as a reminder to internal organizations and customers accepting organizational security certifications that certification does not guarantee the security of the subject.

Limitations and Opportunities for Future Research

Limitations of this study include the need for more data on the relationship between certifications and operational security from organizations of all sizes across different industries. There is limited academic research on the successes and challenges that organizations experience while working towards successful organizational security certification. Research is even more limited when considering frameworks typically implemented in United States federal systems, such as NIST or FedRAMP, likely due to the sensitive nature of these environments. This study is also limited by the availability of research, which is skewed towards ISO 27001 certification, known to be less technically rigorous than other standards. Future research should focus on gathering more data from the perspective of organizations to better understand the negative impacts on operational security that they may experience in their journey toward certification. As more research is added to the body of knowledge, the ability to understand and anticipate potential negative impacts of security certifications on operational security can be greatly improved.

References

Andersson, A., Hedström, K., & Karlsson, F. (2022). Standardizing information security–a structurational analysis. *Information & Management, 59*(3). https://doi.org/10.1016/j.im.2022.103623

Beckers, K., Côté, I., Fenz, S., Hatebur, D., & Heisel, M. (2014). A structured comparison of security standards. *Engineering Secure Future Internet Services and Systems*, 8431, 1-34. https://doi.org/10.1007/978-3-319-07452-8_1

Breier, J. (2014). Security Evaluation Model based on the Score of Security Mechanisms. *Information Sciences and Technologies Bulletin of the ACM Slovakia, 6*(1), 19-27.

Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information and Management, 52*(4), 385–400. https://doi.org/10.1016/j.im.2014.12.004

Fomins, V., de Vries, H. J., & Barlette, Y. (2008). ISO/IEC 27001 Information system security management standard: exploring the reasons for law adaptation. Retrieved February 12, 2023, from https://hdl.handle.net/20.500.12259/37814

Freeman, E. H. (2007). Holistic Information Security: ISO 27001 and Due Care. Information Systems Security, 16(5), 291–294. doi:10.1080/10658980701746478

Glaser, B. G., & Strauss, A. (1967). *The discovery of grounded theory: Strategies for qualitative research.* New York, NY: Aldine Publishing.

Hampton, C., Sutton, S. G., Arnold, V., & Khazanchi, D. (2021). Cyber Supply Chain Risk Management: Toward an Understanding of the Antecedents to Demand for Assurance. *Journal of Information Systems, 35*(2), 37–60. https://doi.org/10.2308/ISYS-19-050

Hsu, C., Wang, T. & Lu, Al. (2016). The Impact of ISO 27001 Certification on Firm Performance. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 4842-4848. https://doi.org/10.1109/HICSS.2016.600

IBM (2022). *Cost of a data breach 2022*. IBM. Retrieved October 12, 2022, from https://www.ibm.com/reports/data-breach

ISO (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection, Information security management*. ISO/IEC. Retrieved February 12, 2023, from https://www.iso.org/standards.htm

Jones, K. (2004). Mission drift in qualitative research, or moving toward a systematic review of qualitative studies, moving back to a more systematic narrative review. *Qualitative Report, 9*(1), 94-111. https://doi.org/10.46743/2160-3715/2004.1939

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International journal of information management, 23*(2), 139-154. https://doi.org/10.1016/S0268-4012(02)00105-6

Morrison, A., & Kumar, G. (2018). Corporate Boards May Be More Likely Than Regulators to Scrutinize Cybersecurity Program Effectiveness This Year. *Journal of Health Care Compliance, 20*(4), 49–52.

National Institute of Standards and Technology (NIST). 2018. *Special publication 800-37, revision 2: Risk Management Framework for Information Systems and Organizations.* https://doi.org/10.6028/NIST.SP.800-37r2

Poehlmann, N., Caramancion, K. M., Tatar, I., Li, Y., Barati, M., & Merz, T. (2021). The organizational cybersecurity success factors: an exhaustive literature review. *Advances in Security, Networks, and Internet of Things: Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20*, 377-395. https://doi.org/10.1007/978-3-030-71017-0_27

Prislan, K., Mihelič, A., & Bernik, I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. *PloS one, 15*(9), e0238739. https://doi.org/10.1371/journal.pone.0238739

Rahman, M. R., & Williams, L. (2022). An investigation of security controls and MITRE ATT&CK techniques. *arXiv preprint arXiv,* 2211.06500. https://doi.org/10.48550/arXiv.2211.06500

Razikin, K., & Widodo, A., (2021). General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance. *CommIT Journal, 15(*2), 91–104. https://doi.org/10.21512/commit.v15i2.6931

Sharma, N. K., & Dash, P. K. (2012). *Effectiveness of iso 27001, as an information security management system: an analytical study of financial aspects. 9*(3).

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems, 44.* https://doi.org/10.1016/j.accinf.2021.100548

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An Instrument for Evaluating the Effectiveness of Enterprise Information Security Programs. *Journal of Information Systems, 30*(1), 71–92. https://doi.org/10.2308/isys-51257

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020). MITRE ATT&CK: Design and Philosophy. Available at: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Vance, A., Siponen, M. & Pahnila, S. (2012). Motivating is security compliance: insights from habit and protection motivation theory. *Information & Management, 49*(3/4). https://doi.org/10.1016/j.im.2012.04.002

Verizon. 2022. Data Breach Investigations Report. Available at: https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii-xxiii. http://www.jstor.org/stable/4132319