Information Security Posture to Organize and Communicate the Information Security Governance Program

Dinh Uy Tran (https://orcid.org/0000-0001-5691-7641),
Audun Jøsang (https://orcid.org/0000-0001-6337-2264)
University of Oslo, Oslo, Norway
dinhut@ifi.uio.no
josang@ifi.uio.no

Abstract: Information security practice has evolved greatly from being mostly a technical concern to also becoming a concern of executive management. As a result, there are many different frameworks, guidelines and certification programs for information security governance (ISG) and management. The purpose of these standards and certification programs is to help an organization develop a structured approach for governing and managing information security. However, these standards and guidelines are generic and not tailored for any specific organization. These frameworks usually specify *"what"* should be implemented but not *"how"*. Additionally, these frameworks do not specify *"how"* to communicate the information security posture (ISP) to the executive management in a simplistic manner. This paper first defines and conceptualizes the term *information security posture*, and then proposes a framework on *"how"* to communicate and organize the ISP. Our contribution complements ISG programs adopted by organizations to give executive management a better understanding and oversight. We argue that describing the ISP of an organization will support well-informed decision-making while ensuring alignment with business objectives.

Keywords: Information Security Posture; Information Security Governance; Information Security Management; Information Security Reporting; Risk Management; Information Security Program

1. Introduction

Information security is a topic that receives increasing interest from top-level management. The reason why information security risk has evolved from being mostly a technical concern to becoming a priority for management is that an information security breach could have dire consequences for an organization. It is necessary that ISG (Information Security Governance) is structured in a way that gives an organization oversight over its ISP (Information Security Posture), because this understanding is essential to ensure alignment with business objectives. The term ISP is widely used in the literature but is often interpreted inconsistently because of the lack of standardization. Based on these identified issues this paper discusses three research questions (RQ), as described in table 1:

RQ1: *What is information security posture from a holistic perspective and what should it consist of?*	**RQ2:** *How to organize the information security governance program and improve the information security posture?*	**RQ3:** *How should the information security posture be communicated to executive management, and be used for better decision-making?*

Table 1. Research questions

It is necessary to get a better understanding of how we want to understand ISP before investigating how it can be leveraged. After achieving an understanding of what it should be by making the term more meaningful and useful, then it is possible to describe more in detail what components it should consist of. On this basis it will be possible to explain, organize and communicate what ISP is, and how to improve the posture.

This paper is structured as follows. The theoretical background which gives an introduction to this topic is described first. Next, we describe how the collected research papers were analyzed and compared. Then, the results of our findings are presented. Finally, the paper ends with a discussion on limitations, suggestions for future research and concluding remarks.

2. Background

The purpose of this section is to give a brief description of ISG and ISP.

*Published at the 18th European Conference on Management Leadership and Governance, ECMLG 2022, pp 515-522, DOI: https://doi.org/10.34190/ecmlg.18.1.729

2.1 Information Security Governance

There are several different interpretations of what ISG is, but they typically have some core similarities. The common agreement among researchers is that ISG should not be seen as a technical matter, but rather as a business matter and a subset of corporate governance (Soomro *et al*., 2016; Von Solms & Von Solms, 2006; Pérez-González *et al*., 2019; Posthumus & Von Solms, 2004). This underlines the importance of implementing a holistic ISG program that includes human, process, physical and technical issues. In addition to the above-mentioned elements, Slayton (2021) expresses the importance of establishing a "chain of trust" in supply chain management. This is challenging, since ISG must then cross the boundary of "internal control", and be extended to strategic partners.

The purpose of ISG is for executive management to direct and control information security activities in alignment with business objectives (Posthumus & Von Solms, 2004). This means that executive management needs oversight over the ISG program and must monitor and validate that information security controls are performing according to business objectives (Whitman & Mattord, 2014). Validation is based on collecting measurements and metrics to evaluate the overall effect of the ISG program. Anu (2021) states that developing metrics will help organizational leaders to understand the ISP resulting from the implemented controls and support effective decision-making.

When executive management has obtained oversight and understanding based on knowledge, then according to Slayton (2021), it is possible to direct and manage risk by turning uncertainty into known risk, which in turn forms the basis for selecting information security controls to address and modify the business risk to an acceptable level. It is important to acknowledge that the ISP is not a steady state and that the threat landscape is constantly changing (Williams, 2012). Slayton (2021) argues that the increasing complexity and rapid change in technology result in unpredictability and uncertainty when directing the business, even when an ISG program is implemented. An example of complexity is when an organization has interdependencies with other organizations/suppliers. Broadening the scope of the ISG program to address business partners can help an organization turn uncertainty into a known risk and also make an organization more resilient against unknown risk. This means that the ISG program needs to be flexible to incorporate dynamic changes in the environment (Soomro *et al.,* 2016).

The importance of ISG has led to the development of various standards that can be used for certification to attest an organization's commitment to secure its business (Siponen & Willison, 2009). These standards are developed as the consensus of experts in the field of ISG and management. Based on this, Von Solms & Von Solms (2004) argue that it is unnecessary to spend the effort to "re-invent the wheel" when an organization can "follow a best practice". There are some limitations to Von Solms & Von Solms (2004)'s statement. As an example, Siponen & Willison (2009) argue that there is no evidence behind the claim that there always exists a "best practice". Methods of best practice are not consistently published, and hence there is no evidence of the availability of "best practice". These standards are also generic and not tailor-made according to organizational differences, a fact that conforms to the research of AlGhamdi *et al*. (2020) who concluded that most proposed frameworks are not validated and do not provide any detailed description of how to implement a framework. Even so, there seems to be a common agreement that applying a standard is a good starting point for ISG, and then supplementing with other standards and frameworks to suit the organization (Veiga & Eloff, 2007; Siponen & Willison, 2009; Culot *et al*., 2021; AlGhamdi *et al*., 2020).

2.2 Information security posture

As mentioned earlier the purpose of ISG is to give executive management oversight over the organization's ISG program and risk environment. This can be achieved by monitoring the ISP. Whitman & Mattord (2014) and Veiga & Eloff (2007) use the term oversight/oversee, while Young (2008), Johnston & Hale (2009) and Anu (2021) use the term ISP, but we argue that they should be interpreted as being equivalent. While the terms can be discussed at different management levels, it can be argued that for the communicational purpose it is beneficial to standardize and use the term ISP instead of oversight/overseeing the ISG program. The reason for preferring to use the term ISP is that it gives management an indication of what is discussed instead of being something they should oversee. Both Johnston & Hale (2009) and Anu (2021) argue that by monitoring ISP, an organization can indicate the alignment of business objectives, but neither defined what ISP should be. Williams (2012) has defined ISP as an indication of the countermeasures against threats implemented to protect the organization's resources, while Young (2008) gives a similar definition, which states that it is the current organizational state in activities, interaction and integration of information security objectives. Young (2008)'s definition is also compliant with NIST (2022), which defines ISP as the security status of an enterprise's networks, information,

and systems based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

The resemblance between the definitions is related to the current state/status of the information security controls, and hence it could be argued that it should instead be called information security status. NIST (2022) has defined ISP as synonymous with security status. However, the literature does not discuss how to assess the ISP or how the aggregation of measurement data flows. Based on these definitions, we attempt to add more meaning to the term and supplement the contribution proposed by Young (2008), Williams (2012) and NIST (2022).

3. Method

This research method is based on Kitchenham (2004)'s procedure for Systematic Literature Review and is supplemented with coding concepts from the Grounded Theory (Mills *et al*., 2006). This research has been conducted according to figure 1 and is further explained below.

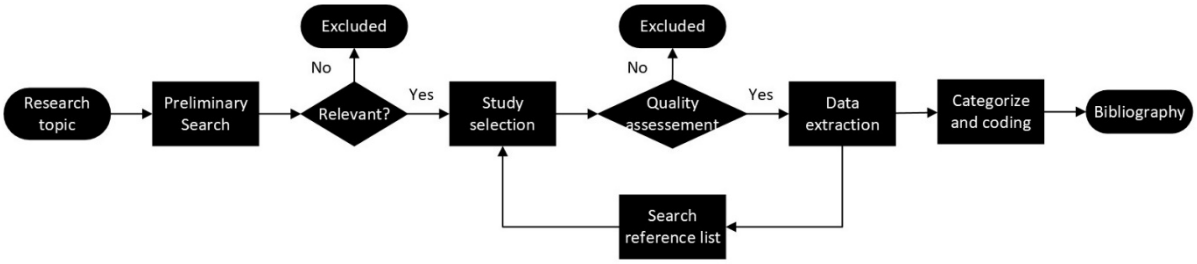

Figure 1. Research method

The research topic was identified based on our own work experience and as the main motivating factor. Two types of search engines were used, here defined as "primary" and "secondary" search engines. The primary search engine is for collecting relevant research papers, which constitute our preferred source. The secondary search engine is for collecting non-research papers, for instance relevant frameworks, guidelines and "best practices" which are supplementary data.

The primary search engine is Google scholar, while ORIA was used to collect relevant research papers, which is a library software from the University of Oslo. The search strings that were used in the preliminary search were: *"Information security posture"* with 16 400 hits, *"Cyber security posture"* with 4820 hits, *"Security posture"* with 5960 hits, *"Information Security Governance"* with 17 800 hits, *"Cyber Security Governance"* with 16 200 hits, *"Information Security Management"* with 42 600 hits, *"Information Security Management System"* with 25 700 hits and *"Information Security Reporting"* with 27 600 hits.

The Secondary search engine consists of ISO, NIST, NSA, ISC^2 and ISACA, which are well known for certifications and developing standards. The search strings were only *"information security posture"* because they mostly provide standards and material on information security governance and management, but not research papers: The findings are ISO (2 hits), NIST (1079669 hits, but without the ability to filter), NSA (40 hits), ISC^2 (1 hit) and ISACA (61 hits). Non-relevant papers were excluded from this research based on the title, abstract and keyword in the preliminary search.

The preliminary search phase covers all search strings mentioned above except for "posture" on research papers published in 2021 and 2022. The main reason is that we wanted the most up-to-date research because there are many papers on ISG and management. Then we reviewed the reference list from these papers to identify more relevant papers. "Posture"-related strings were searched with "any time" and the findings were sorted from newest papers to older ones. We used a broad timespan on "posture" because there is less research literature in this area, and we wanted to ensure we could find all relevant papers. The result was that 17 research papers and 1 journal/article from secondary search engine were deemed relevant by reading the title and abstract. We developed inclusion-exclusion criteria (provided in Table 2) to assess the quality and relevancy.

Inclusion	Exclusion
Papers that define Information security posture	Papers unrelated to our research topic
Papers that indirectly explain or define information security posture	Papers that contain search strings but do not explain the terms
Papers that explain the characteristics of information security governance	Papers that are not in English
Papers describing a framework for information security governance	

Table 2. Inclusion-exclusion criteria

The inclusion-exclusion criteria were applied, and the final list consist of 6 relevant papers. To extract data, we populated a form containing extracted relevant quotes and explanations from different papers. Then we used a concept from the Grounded Theory research method, which consists of developing codes or key concepts from extracted data used for theoretical analysis and identifying core categories (Mills *et al*., 2006). Then, we could use the codes to discover, compare and correlate with different categories. We used this concept to get a better overview of the surveyed research. We defined 10 core categories with corresponding codes and noted which and how many of the research papers discussed those categories. Some codes are identical or similar in different categories and the logic is to make it easier for us to discover interconnections between different categories even though they are discussed directly/indirectly by different papers.

By reviewing the reference list and data extracted from relevant research papers we identified additional 17 research papers relevant for this research and did another iteration, which identified 11 more papers. After verification of the relevancy, we ended up with 16 research papers and 1 journal article related to ISG, management and ISP. Finally, all relevant papers are listed in the bibliography.

4. Results

This section describes the results from analyzing data extracted from the systematic literature review and presents answers to the three research questions.

4.1 RQ1 - What is Information Security Posture from a holistic perspective and what should it consist of?

The first aspect that needs to be discussed is whether ISP should be defined as just the status of the information security activities in an organization. Both Young (2008) and NIST (2022) state that it is the status, but Williams (2012) does not use the term status but an “indication” of implemented security controls. By using the term indication it could be interpreted as saying that there is still uncertainty and that there are unknown aspects of the implemented controls, a view also supported by Slayton (2021). There seems to be a consensus that ISP consists of the status of the implemented security controls. We argue that both status and uncertainty must be addressed as components of ISP. The difference between a posture and status is that a posture is more dynamic, while status is more static. Information security is as Williams (2012) argues not a steady state because of the evolving threat and risk landscape. Simply understanding the current state is not enough to have a holistic understanding of ISP. We argue that organizations also need the component of being able to prepare for ever-changing threats and risk landscapes to reach a “potential future state”. By adding this component to the definition, then it can address both known unknowns and unknown risks. Without this component then ISP is limited to known knowledge, which simply could be defined as status.

It can be argued that the basis of ISP is the combination of “current state”, “uncertainty” and “potential future state”. Even so, there is an intersection between “potential future state” and “current state” because these components depend on each other in the sense that preparing for the future state needs the understanding of the current state of implemented security controls. By including uncertainty is to acknowledge unpredictability that arises with regard to risk. It must also be communicated to executive management that ISP is dynamic because of the rapid change in the threat and risk environment.

Based on the discussed definitions from Young (2008), Williams (2012) and NIST (2022) it can be argued that their definitions give different perspectives on the ISP. For instance, the definition from NIST (2022) starts with the status of the organization’s network and information systems which clearly is seen from a technical perspective. Williams’ (2012) definition focuses more on the infrastructure security posture and Young’s (2008) view is that ISP consists of controls related to recovery, deterrence, detection and prevention. It can be argued that all of these perspectives are correct because they are discussed at different management levels.

Management levels can indicate a reporting structure and how measurement data aggregates. The meta-study by AlGhamdi *et al*. (2020) shows that reporting is a critical success factor for good ISG practice, e.g. because it improves decision-making. Among the 14 studies that were evaluated by AlGhamdi *et al*. (2020), 2 studies had been validated and the remaining studies suggested the importance of reporting based on prominent frameworks or their own research. Even so, the 2 validated studies did not specify the quality of the validation process.

Even if there is little-validated evidence that a reporting structure is a critical success factor, it is obviously needed so that executive management can have oversight over the ISP. Based on our findings from Young (2008), Williams (2012) and NIST (2022) who discuss ISP at different levels, and from AlGhamdi *et al*. (2020) who discussed the importance of reporting, it can be argued that there are different posture levels depending on the ISG program, which in combination underlines a reporting structure. This is why we propose that the definition should include different levels of ISP that in total give the executive management a holistic oversight. Based on the discussion above, we define the overall ISP as follows:

"*The information security posture is the current and predicted future state of information security based on a structure for continuous monitoring and oversight over the current state of an organization's security controls (organizational, technological and physical controls) and the constantly changing risk environment for predicting the potential future state. The purpose of continuously monitoring and evaluating the information security posture is to be informed about the information security status with related uncertainties, to understand how well it currently supports business objectives and how it can be adjusted to better support business objectives in a changing threat landscape and business environment.* The information security posture is conceptualized and illustrated in figure 2.

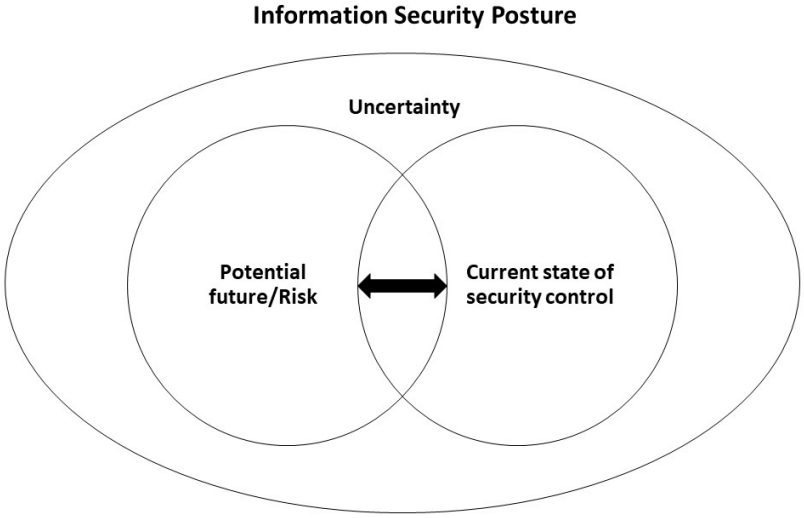

Figure 2. Conceptualization of Information Security Posture

4.2 RQ2 – How to organize the information security governance program and improve the information security posture?

The papers mentioned earlier state that reporting is a critical success factor, but none of them specify "how" to organize a reporting structure. We therefore propose a concept, which is adaptable to different organizations. We also break down the concept of ISP into separate levels, to make it more manageable for instance to conduct a capability maturity assessment on different levels of ISP, which in turn determines the overall ISP.

The main difference between ISP and the maturity level of information security management is that ISP also addresses the degree of alignment with business objectives. Improving the maturity level does not necessarily lead to an improved posture level, since a mature security control/process might not be well aligned with business objectives. Hence, maturity assessment is one of the many tools used to improve ISP. Since the ISP consists of different levels, then each level must be defined to have the same common ground for discussions. We have defined the management level as suggested by Von Solms & Von Solms (2006) with three sub-level: Strategic, tactical and operational.

The strategic level represents the overall ISP. It sets the basis for directing all management levels while receiving compiled reports from the tactical level. The accumulation of reports gives the executive management oversight over to which extent the organization is aligned with business objectives, which is used to improve decision-making.

The tactical level consists of two key components: the potential future state by risk management and the current state of security controls. The tactical level receives direction from the strategic level and directs the operational level by enforcing policies and receiving measurement data about conformance. The component "current state of security controls" is determined by collecting data from different sources based on all types of security controls, which can be organizational, technological and physical. The component "potential future state by risk management" is determined by assessing potential risk based on data from the "current state" and the predicted future threat landscape. It is important to address all elements of risk like adversarial threats, natural occurrences, human-related incidents and opportunities (Posthumus & Von Solms, 2004). Then, the tactical level compiles all measurement data from the two key components into a report which is submitted to the strategic level.

The operational level consists of the individual security controls grouped by organizational, technological and physical types. The operational level receives direction from the tactical level, executes according to policy and produces measurement data indicating the conformance level. The most important aspect is that every security control must address people, process, technology (Posthumus & Von Solms, 2004; Veiga & Eloff, 2007) and suppliers (Slayton, 2021; Culot *et al*., 2021), which gives a holistic understanding of the ISP. Every organization is different, and not everyone who works with access control is organized in the same department, and hence may have different managers; this is what Palmberg (2009) refers to as the functional groups. To address this issue, it is necessary to remove barriers between functional groups by organizing cross-functional team members, which Palmberg (2009) defines as process management. By organizing processes, it is necessary to define roles, and most importantly to avoid that process owners have conflicting authority with functional group leaders. Process owners are accountable for their respective processes and must ensure alignment with defined policies. This means that the process owner must oversee performance measurement, ensuring continuous improvement and the desired posture level by leading members in the process team (Palmberg, 2009).

4.3 RQ3 - How should the information security posture be communicated to executive management, and used for better decision-making?

We have discussed how to organize a reporting structure, but even so there is no widely accepted method on how to report. Below, we propose some reporting concepts and define criteria for different ISP levels corresponding to categories. An example is provided in table 3:

Colour code	Posture category	Criteria
White	Excellent posture	80%-100% conformance
Green	Good posture	60%-79% conformance
Yellow	Moderate posture	40%-59% conformance
Orange	Poor posture	20%-39% conformance
Red	Critical posture	0%-19% conformance

Table 3. Posture levels and criteria

By using posture criteria, a process manager can assign a posture level to the ISP they are accountable for. The conformance is determined by an average score from the metrics collected from different postures according to a pre-set baseline. This sets the basis for decision-making since it can be used to discuss which posture should be prioritized to reach a higher conformance level, or it can be used for identifying risk. Since each posture consists of data about conformance levels and is organized in a manner that can aggregate to different management levels, it is possible to discuss it on any level. This model can be integrated into a dashboard, which automatically monitors and collects measurements. By implementing a dashboard, the executive management has oversight and can oversee the ISG program.

As already discussed it is important to address uncertainty, where an example is provided in table 4. The uncertainty assessment should be used in conjunction with posture-level criteria:

Uncertainty level	Confidence level
High	0%-24%
Medium	25%-59%
Low	60%-79%
Minimal	80%-100%

Table 4. Correspondence between uncertainty and confidence levels

The purpose of considering the uncertainty levels is to communicate how confident you are in the data from the ISG program. For instance, if you report a moderate ISP, then you must also state how confident you are in that assessment. Things that can affect the confidence level e.g., the amount and how you collect data, how you process data, method and the validity of the assessment. Understanding the uncertainty means that you acknowledge it and can manage uncertainty to an acceptable level of confidence, which could lead to better decision-making. The principle is that it is unsafe to make important decisions based on highly uncertain ISP assessments.

5. Limitation

While this research contributes by defining, adding more meaning and conceptualizing ISP, it is important to discuss the limitations of this research.

First, regarding the method for collecting data, there is the possibility that the search strings and engines have not been optimal. However, we argue that the quality of data collection was fairly good, because from the reference list the term ISP was mentioned directly and indirectly in 8 research papers, while 2 of the research papers had defined the term, as well as 1 non-research web article. From the initial search, even more research papers mentioned the term ISP, but these articles were irrelevant for this research. There is a possibility that ISP has been discussed and defined by other researchers and it is possible that we could have found more research papers by performing more iterations of data collection. With a data collection period from 17.01.2022 until 24.02.2022, we judged that we had reached what Crang & Cook (2007) defines as the "theoretical saturation". This means that it might be possible to find research papers with similar findings possibly explained in different ways. However, this would probably not result in a significant additional contribution to our research. Another strategy could be to define a new terminology instead of using ISP, to get a new perspective. However, since the term has not been elaborated on and is a widely used term, we found it beneficial to add more meaning and context to the existing term than to define a new term.

Another reason is that very few research papers have discussed how to implement an ISG program so that the executive management can have oversight over all information security activities. From the data collection, we found only theoretical frameworks, and papers discussing proposed frameworks/standards are generic and do not provide any methodical validation. It is possible that the chosen search strings or searching techniques were suboptimal, meaning that there is still a possibility that there are some research papers on this matter that have not been covered.

Finally, the proposed framework for ISP is a theoretical contribution and has not been validated or tested for practicality. Even so, our research expands and elaborates on how to organize an ISG program, supports other researchers' contributions, and it addresses the need for a framework that describes "how" to organize and communicate an ISG program.

6. Conclusion

This research argues that potential future state and uncertainty are also key components for understanding ISP besides status, and discusses how these components can be related and organized. We argue that ISP can be separated into different levels like a reporting structure, which in turn determines the overall ISP. Then, we suggested how to report ISP levels and communicate uncertainty levels. There might still be some limitations in our research, in which case our contribution can form the basis for further research. Potential future research could be to implement this framework by using action research which could be used to learn and improve the framework and elaborate on "how" to organize an ISG program, hence this research is the first step in this journey.

7. References

AlGhamdi, S., Win, K., & Vlahu-Gjorgievska, E. (2020) "Information security governance challenges and critical success factors: Systematic review", *Computers & security, 2020-12,* Vol.99, 102030, doi:10.1016/j.cose.2020.102030.

Anu, V. (2021) "Information security governance metrics: a survey and taxonomy", *Information Security Journal: A Global Perspective, 2021-05-16,* pp 1-13, doi:10.1080/19393555.2021.1922786.

Crang, M., & Cook, I. (2007) *Doing Ethnographies,* SAGE Publications Ltd, London.

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021) "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda", *The TQM Journal, Vol. 33, No. 7, 2021,* pp 76-105, doi:10.1108/TQM-09-2020-0202.

Johnston, A., & Hale, R. (2009) "Improved security through information security governance", *Communications of the ACM, 2009-01-01, Vol.52 (1),* pp 126-129, doi:10.1145/1435417.1435446.

Kitchenham, B. (2004) "Procedures for Performing Systematic Reviews", *Keele University Technical Report TR/SE-0401*.

Mills, J., Bonner, A., & Francis, K. (2006) "The Development of Constructivist Grounded Theory", *International Journal of Qualitative Methods, 2006, 5(1),* pp 25-35, doi:10.1177/160940690600500103.

NIST. (2022) "*NIST Information Technology Laboratory"*, [online], Computer Security Resource Center - Glossary: https://csrc.nist.gov/glossary/term/security_posture.

Palmberg, K. (2009) "Exploring process management: are there any widespread models and definitions?", *TQM journal, 2009-02-27, Vol.21 (2),* pp 203-215, doi:10.1108/17542730910938182.

Pérez-González, D., Preciado, S., & Solana-Gonzalez, P. (2019) "Organizational practices as antecedents of the information security management performance: An empirical investigation", *Information Technology & People, West Linn, Vol. 32, Iss. 5, (2019),* pp 1262-1275, doi:10.1108/ITP-06-2018-0261.

Posthumus, S., & Solms, R. (2004) "A framework for the governance of information security", *Computers & Security (2004) 23,* pp 638-646, doi:10.1016/j.cose.2004.10.006.

Siponen, M., & Willison, R. (2009) "Information security management standards: Problems and solutions", *Information & Management 46 (2009),* pp 267–270, doi:10.1016/j.im.2008.12.007.

Slayton, R. (2021) "Governing uncertainty or uncertain Governance? Information Security and the challenge of cutting ties", *Science, Technology & Human Values 2021, Vol. 46(1),* pp 81-111, doi:10.1177/0162243919901159.

Von Solms, B., & Von Solms, R. (2004) "The 10 deadly sins of information security management", *Computers & security, 2004, Vol.23 (5),* pp 371-376, doi:10.1016/j.cose.2004.05.002.

Von Solms, B., & Von Solms, R. (2005) "From information security to…business security?", *Computers & security, 2005, Vol.24 (4),* pp 271-273, doi:10.1016/j.cose.2005.04.004.

Von Solms, R., & Von Solms, S. (2006) "Information Security Governance: A model based on the Direct–Control Cycle", *Computers & security 25 (2006),* pp 408–412, doi:10.1016/j.cose.2006.07.005.

Soomro, Z., Shah, M., & Ahmed, J. (2016) "Information security management needs more holistic approach: A literature review", *International journal of information management, 2016-04, Vol.36 (2),* pp 215-225, doi:10.1016/j.ijinfomgt.2015.11.009.

Tashi, I., & Ghernaouti-Helie, S. (2009) "A Security Management Assurance Model to Holistically Assess the Information Security Posture", *2009 International Conference on Availability, Reliability and Security, 2009-03,* pp 756-761, doi:10.1109/ARES.2009.28.

Veiga, A., & Eloff, J. (2007) "An Information Security Governance Framework", *Information Systems Management, Fall 2007, 24,* pp 361-372, doi:10.1080/10580530701586136.

Whitman, M., & Mattord, H. (2014) "Information Security Governance for the Non-security Business Executive", *Journal of Executive Education, 2014, 11(1),* pp 97-111.

Williams, G. (2012) "Cost effective assessment of the infrastructure security posture", *7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012, 2012,* p.1B4, doi:10.1049/cp.2012.1503.

Young, R. (2008) "Defining the information security posture: an empirical examination of structure, integration and managerial effectiveness", *University of North Texas, Unpublished PhD Thesis*, [online], https://www.researchgate.net/publication/228413655_Defining_the_information_security_posture_an_empirical_examination_of_structure_integration_and_managerial_effectiveness.