Business Language for Information Security*

Dinh Uy Tran**[1][0000−0001−5691−7641] and Audun Jøsang[1][0000−0001−6337−2264]

University of Oslo, 0373 Oslo, Norway

Abstract. Prominent standards and frameworks for information security clearly state that business aspects on the one side, and technical aspects on the other, are equally important for the management of cyber security. Organisations with a relatively low maturity level in security management typically consider information security primarily as a technological issue. For those organisations, information security might not get the necessary support from top-level management because they are predominantly focused on business aspects, and are blind to the role information security plays for business. To obtain support from top-level management the information security practitioners need the skills to influence and help relevant stakeholders to understand how information security can support business objectives. In this debate, it is often argued that it is important to speak the language of management. This means that information security practitioners should learn how to translate technical terms to a business context, so top-level management can understand what it means for them. However, this debate has mostly focused on the importance of speaking the "Business Language for Information Security (BLIS)" but has not elaborated on what this language consists of and how to learn it. This paper proposes BLIS and a framework for how to learn it. By mastering BLIS, security professionals can articulate arguments that top-executive management can easily understand and act on. Therefore, we argue that taking a learning module on BLIS will be valuable and useful for the next generation of students in information security. Said briefly, learning BLIS will help students understand how information security can support business, and also how this can be explained to others.

Keywords: Business Language for Information Security · Information Security Governance · Information Security Management · Information Security Reporting.

1 Introduction

Information security is receiving increased attention through wide media coverage of hacking and cyber attacks. From these incidents, we learn that "hacking"

* Published at the Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, vol 674. Springer, Cham., pp. 57–68.

** Supported by Sykehuspartner Trust.

can have dire consequences for businesses, and hence is not only a technical issue. Information security needs to be seen both as a business issue as well as a technical one. Top-level management therefore needs an understanding of how information security actually supports business objectives.

The meta-study by AlGhamdi *et al.* [18] suggests that effective management and governance of information security require top-level management support and commitment. Their study is based on a survey of 60 papers where top management support is listed as 1 of 34 critical success factors. This is supported by Soomro *et al.* [16], who based on their meta-study stated that a lack of top-level management support reduces the effectiveness of information security efforts in an organisation. The authors argue that information security managers should involve top-level management while adopting a holistic approach to information security. This is precisely one of the requirements expressed by ISO/IEC 27001:2022 [35], which is a well-recognized standard for establishing an Information Security Management System (ISMS). Requirement 5.1 from ISO/IEC 27001:2022 [35] specifies that top management shall demonstrate leadership and commitment to the ISMS. A risk report from the The Directorate of e-health [36] under the Norwegian Ministry of Health and Care, stated that 88% of public healthcare institution have established an ISMS. The report also states that 22% of security incidents occur because of the lack of prioritisation of information security work, 33% of incidents occurred due to the lack of security processes, and one third of all public institutions detects security incidents by accident. Basically, these 88% of the health care institutions having implemented an ISMS should have top management support, but security incidents still occur because of the lack of prioritisation. This could indicate that the top management does not understand how information security can support the business, which is quite alarming when the national strategy for digital security in Norway [37] requires that organisations adopt well-known standard in ISMS such as ISO/IEC 27001:2022 [35].

The main motivation for this research is to overcome the difficulty that security specialists have in communicating how information security supports business objectives. The goal of understanding and explaining how information security supports business is to ensure that information security gets adequate prioritisation, and that management commitment is not simply signing off the ISMS documents without any real commitment. Researchers such as Karanja [13], Jirasek [14], and Johnston *et al.* [17] argue that information security management practitioners should talk the same "language" as that of top-level management and communicate in a clear and simple way how information security is aligned with business objectives. However, these researchers do not discuss how this "security business language" can be learned and used to influence top-level management to obtain support and commitment.

This research proposes a method for communicating information security in way the top management understands and hence results in management commitment. Our observation is that many researchers discuss this topic either directly or indirectly, and that the term "Business Language" is commonly used by both

researchers and practitioners. For the present paper, we will use the term "Business Language for Information Security", for which we also provide a definition. Then, we will discuss what BLIS should consist of, which represents the theoretical framework for learning BLIS. This paper starts with a brief review of related research on this topic. Next, we describe the research method and how collected papers were analyzed and compared. Then, the results and discussion of the findings are presented. Finally, the paper provides some concluding remarks and proposes ideas for future research.

2 Background and related research

Information security researchers and practitioners have acknowledged the importance of communication skills to make information security understandable for top-level management. Whitman & Mattord [12], Jirasek [14], Fitzgerald [20], Harkins [22], and Johnston *et al.* [17] argue that information security practitioners should speak the language of business in a way that top-level management can easily understand. Schinagl & Paans [7] argue that experts tend to articulate their technical knowledge in a way that non-experts find difficult to grasp, while for peer experts, the same way of articulating technical issues is self-evident. Such cases of "system language" are typically used and understood within a group of experts, but represent a barrier to understanding for outsiders. Translating the system language of information security into business language will help non-experts understand how information security affects business. Karanja [13] also uses the term "business language" to describe the same matter. Researchers such as Ashenden & Sasse [15, 1], Soomro *et al.* [16], AlGhamdi *et al.* [18], and Rainer *et al.* [11] argue that effective communication is needed to ensure a common understanding between Information Security managers and top-level management.

There is a general consensus between researchers discussing communication, the language of business, and business language. However, it is often the case that researchers use different terms to discuss the same topic, which can lead to confusion. The lack of a standardised definitions is typically the root of the problem, which makes it necessary for practitioners to learn that different terms often mean the same thing. In this paper, we use the term "Business Language for Information Security". As mentioned, the concepts that BLIS covers have been mentioned by different researchers, but we have not found any publication elaborating specifically on the interpretation of BLIS and how it can be applied. For instance, what is the business aspect of BLIS? What communication skills should be a part of BLIS in a way that is useful for communicating with top-level management? Our observation is that publications indirectly mentioning BLIS are related to Information Security Governance (ISG), Information Security Management (ISM), and the role of the Chief Information Security Officer (CISO). Unsurprisingly, these topics are related to business, and the CISO is usually a part of top-level management, or acts as an advisor related to information security. Understanding ISG, ISM, and the role of CISO provides the

basis for defining what BLIS should consist of. A clear definition of BLIS and a method to learn it will prepare the next generation of students for working on information security in business settings.

The purpose of ISG is to establish a governance structure for top-level management to direct and control information security activities to support business objectives (Posthumus & Solms, [25]). This means that ISG is a tool for CISO to get oversight over the information security activities and how they perform according to business objectives, also known as information security posture (ISP). By monitoring the ISP, the CISO has oversight over risks, uncertainties, and the status of the ISG program and can use this insight to ensure that top-level management takes well-informed decisions (Tran & Jøsang, [31]). To ensure that ISG is aligned with business objectives, the CISO needs to manage personnel, processes, and technology related to Information Security by overseeing and managing daily security activities, which is known as ISM, and is an integral component of ISG (Solms & Solms, [26]).

Ashenden [15] argues that ISM is about managing people, since people are the ones who use processes and technologies to achieve business objectives. When dealing with the human aspects of management, it is beneficial to have an understanding of different fields of management, organisational behaviour, and culture. Soomro *et al.* [16] suggest that ISM requires a good understanding of organisational structure to facilitate reporting structure, clear authority, and efficient communication and processes. To manage people, it is beneficial to develop leadership and interpersonal skills for motivating and influencing people, but also for effectively communicating with top-level management (Whitten, [21]). Relevant research indicates that for BLIS to be effective, it should include elements from business, leadership, soft skills, communication, ISG, and ISM.

3 Research method

A systematic literature review based on a procedure developed by Kitchenham [30] was conducted and split into two phases. The first phase was to collect papers related to BLIS from three digital libraries, while the second phase consisted of identifying additional papers based on analysing selected papers from the first phase. The chosen digital libraries were Scopus, Web of Science, and Google Scholar, which include a vast amount of papers on different areas of Information Security. The search keywords used are: "Business Language for Information Security", "Business Security Language" and "Business Language for Cyber Security". The search was conducted in September 2022, and the results were sorted based on relevancy. To the best of our abilities, there is no prior research specifically on what we call Business Language for Information Security. The search returned from the first phase is provided in table 1:

We then screened the title and abstract accordingly to identify papers that could discuss the topic, which identified 32 papers for which we conducted a full-text assessment. During the full-text assessments, we applied principles from Grounded Theory (Mills *et al.*, [29]) because there is no prior research on BLIS.

Table 1. Data collection - BLIS.

Search keywords	Web of Science	Scopus	Google Scholar
"Business Language for Information Security"	542	855	3520000
'Business Security Language"	1173	1708	3550000
"Business Language for Cyber Security"	66	91	274000

In the Grounded Theory, a researcher seeks to construct a theory from examining data, while the researcher has limited knowledge or only few predetermined ideas. Because of the limited literature on BLIS, Grounded Theory was suitable for this research as a method to generate new ideas and gain better understanding of this topic.

During the full-text assessments, comparing similarities from different contributions by different researchers we could identify common characteristics, and started to translate these findings into codes and categorizations. This in turn helped us generate and refine our research questions, and we developed inclusion and exclusion criteria to help us identify relevant research papers. The inclusion and exclusion criteria were constantly evolving until we reach the point of theoretical saturation (Crang & Crook, [32]). Saturation means that we had reached a point where we could possibly collect additional similar findings, but that simply explain the same concepts and ideas in different ways, which would not likely contribute more to our research.

The initial step when conducting a full-text assessment with principles from Grounded Theory was to generate open coding (Glaser, [33]), which is a theoretical analysis from the research data and why these are relevant to this research. Which in turn resulted in 47 open codes, this forms the basis to identify core categories. These five core categories are Business, Communication, Information Security, Soft Skills, and Pedagogy. Then, we transferred the open codes to their respective categories.

Both the core categories and open codes functions as our inclusion and exclusion criteria's, for identifying relevant papers. Afterwards, we used another form of coding called axial coding (Strauss & Corbin, [34]) to make links between the open codes and core categories. These links are used to identify interconnections and if these topics are discussed directly or indirectly by other researchers. To link these codes together, we used a diagramming tool, Obsidian to give us an oversight over the complex interplay from the different researchers, which could aid us in our research.

A result of the full-text assessment from the 32 papers, only 24 of these papers were relevant. However, based on the first iteration, we identified 12 additional papers from our initial full-text assessment and then performed the same research procedures on these papers. We decided that it was only needed to perform the research procedure twice, since our observation is that we found the same results but explained differently, hence theoretical saturation as discussed earlier.

This resulted that 36 papers and 47 codes were deemed relevant for BLIS. The core categories are Business (13 codes), Communication (13 codes), Information Security (8 codes), Soft Skills (8 codes), and Pedagogy (5 codes). After two iterations of this research method we could find the gap of existing research on BLIS. Based on these limitations this papers will discuss two research questions:

1. What should the definition of Business Language for Information Security be?
2. What should the theoretical framework for learning the Business Language for Information Security consist of?

3.1 Potential weaknesses of study

Potential weaknesses of this study are related to data collection and developing codes, because only one of the authors was involved in this process. This means that we could have missed relevant research papers that potentially are related to BLIS. However, to address this weakness, we paid attention to the use of databases with most relevant papers and perform the same keyword searches on all databases. Then, we developed codes with corresponding categories to establish an include and exclusion criteria to provide a consistent method of data collection. We argue that the quality of data collection was fairly good, and that the identified 36 papers discuss elements directly or indirectly related to BLIS, and we reached the point of theoretical saturation, as mentioned earlier.

Another potential weakness could be related to defining the different core categories, which later becomes the main components of the theoretical framework for BLIS. Another researcher who performs the same research method would most likely develop different core categories. Which is natural since every researcher has different backgrounds and experiences, which could lead to different views and interpretations. This paper is to the best of our knowledge the first to argue the need for BLIS and present a theoretical framework to learn, and every innovation needs a start and then refined over time. However, to address this weakness, we have to the best of our abilities tried having limited predetermined ideas as possible before the research and let the research data generate a new theory, which is why we used the grounded theory.

A potential minor weakness of this study is our assumption about management commitment from the healthcare sector in Norway, which based on the report [36] was assessed to not give priority to security. Our study indicates that the top management have a relatively limited understanding of how information security supports business objectives. We acknowledge that there could be other reasons for that, like e.g., the health institution has done risk assessments with the conclusion that security should not be prioritised. However, these aspects are not discussed in this study, and there could also be differences in other sectors and countries. Based on our research, we argue that there is a need for helping top management in organisations to understand how security supports the business, which could lead to improved management commitment. Most literature and standards discuss the importance of management commitment, but not

how to gain that commitment, which is precisely the focus of the present study. Either way, if our assumptions about the report is correct or not, this research can give professionals better awareness about the business side and increase the likelihood of gaining top management commitment.

4 Results

This section describes our critical analysis of collected papers and presents our results.

4.1 Definition

From the relevant papers, we observe that the common element of BLIS is that information security practitioners should speak the same language as business practitioners. We agree that one of the outcomes of BLIS is related to "speaking the same language as business people" or "translating technical language to business language", but we argue that it is not only for communications. We find translating "technical language to business language" more precise than "speaking the business language".

We argue that the aim of BLIS is not just to speak the business language, but to make others understand the importance of information security for business. Primarily, it is absolutely necessary to understand relevant business fields. Secondly, information security practitioners should have solid competence in relevant information security fields. Having solid competences should help practitioners have a better foundation to translate the information security language into business language in a way that is simple to understand. Thirdly, it is important to have learned the basic elements of communication science, which includes soft or interpersonal skills, but we added soft skills as a fourth aspect to emphasise its importance. Finally, it is also about learning pedagogy to teach and merge these components practically and efficiently.

These 5 components of BLIS are what we discovered by conducting full-text assessments, and we argue that it is necessary to learn all these components to master BLIS. We argue that learning BLIS can help the next generation of practitioners get a better understanding of skills needed to improve and understand how information security supports business, and develop communication strategies with the help of soft skills for different target users and not limited to top-level management. Pedagogy is to learn how to teach different aspects of BLIS and is not limited to speaking the business language.

We therefore, argue that BLIS is a distinct field within information security that is essential for effectively managing information security in a professional business setting. Based on the discussion above, we define BLIS as follows:

"Business Language for Information Security is a field that merges relevant fields from Business, Communication, Information Security, Soft Skills and Pedagogy for practical use of Information Security in a professional business setting"

We argue that this definition captures all the relevant aspects of BLIS, and is not limited to communicating with top-level management. We argued that BLIS is a distinct field within information security, and is applicable for many use cases. To effectively practice BLIS, a structured approach to learning is needed for merging the 5 elements it contains. It needs dedication to learn BLIS, which cannot be compared to simply "speaking" the business language. Also, we could have given a new definition instead of using BLIS, but we found it more beneficial to add more meaning and make the existing term more useful. Next, we will discuss the content in the 5 key components of BLIS.

4.2 Business and Information Security

To identify relevant business fields, we must analyse fields in information security that have an intersection with and identify different use cases in which an information security manager can be involved with top-level management. Fields like ISG and ISM are well established through numerous standards, and a consensus among researchers is that ISG is a subset of Corporate Governance (Posthumus & Solms, [25]; Soomro *et al.*, [16]). This indicates that it is beneficial for Information Security practitioners to learn about Corporate Governance, which also includes Corporate Risk Management. The same can be said about ISM, which is a subset of ISG and Corporate Governance that it can be beneficial to learn management fields since we are dealing with managing people from different parts and fields in an organisation, not limited to Information Security practitioners. Whitten [21] suggested researching the connections between Mintzberg´s [27] managerial work roles with the CISO role and our observation is that it is relatable. Mintzberg´s [27] defined three manager roles; Interpersonal, Informational, and Decisional, and each role has separate sets of managerial activities. CISO should learn to motivate, develop relationships with other co-workers and build working relationships with other managers through interpersonal contact to ensure effective ISM and organisational culture, which is aligned with Mintzberg´s [27] description of "Interpersonal role".

Soomro *et al.* [16] and Ashenden & Sasse [1] argue that competence in organisational structure is important to facilitate efficient workflow and a reporting structure. AlGhamdi *et al.* [18] argue that information security requires establishing cross-organisational collaboration and can be interpreted as there is a need for competence in process development, which is a view supported by Whitman & Mattord [12], Karanja [13] and Jirasek [14]. Having competence in organisational structure and process development can help CISOs develop effective security metrics, which Anu [19] argues could enable monitoring the overall success of the ISG program. Monitoring and having oversight over information security activities from the ISG program is similar to Mintzberg´s [27] description of the "Informational role".

Finally, a CISO supports top-level management in decision making and devises strategies to achieve business objectives and can act as a negotiator by developing business cases (Rainer *et al.* [11]) to gain needed resources, which is similar to Mintzberg´s [27] description of "decisional role". Johnston *et al.* [17]

argue that it is important to develop interpersonal skills to understand different personality characteristics, and in a management context, we know that every person is different and managers should learn to use different management roles depending on the situation. Hersey *et al.* [28] have developed a framework called "Situational Leadership" to manage different types of persons or stakeholders, which can be useful to handle interpersonal contact.

4.3 Communication and Soft Skills

The field of communication, which includes soft skills or interpersonal skills is related to practicing management as we discussed, but not limited to management, as it applies to other types of people as well. As discussed earlier, the purpose of communication skills is to create a common understanding (Whitman & Mattord, [12]; Ashenden & Sasse, [1]; Harkins, [22]; Hooper & McKissack, [23]). Common understanding can be obtained from "speaking the same language as recipients" (Johnston *et al.* [17]), but also includes other methods like process modelling and rhetoric.

According to Moyón *et al.* [10], process modelling is a visual description to make information security easier to understand for non-security practitioners. For instance, Moyón *et al.* [10] translated a complex security requirement from IEC 62443-4-1 standard into Business Process Modelling Notation (BPMN), which is a type of process model. Then, they interviewed 16 industry experts, of which 14 claimed that the BPMN was easier to understand. This indicates that process modelling can be useful for communicating and unsurprisingly, there are different models for different purposes like the following: Unified Model Language (Sechi *et al.*, [9]), SecureBPMN (Brucker, [5]; Alotaibi, [4]; Altuhhova *et al.* [6]) and Enterprise Architecture Management (Abbass *et al.*, [8]).

Johnston *et al.* [17] argue that learning the field of Rhetoric can be useful to improve the understanding of information security to non-experts. Rhetoric is the practice of communicating a tailor-made message to the recipient, to persuade them to perform a specific set of behaviours or activities. Design tailor-made messages require an understanding of personality characteristics, behaviour, and social skills to interact with different people (Kayworth & Whitten, [24]).

There are different rhetorical techniques, where e.g. the security industry tends to use "fear" to sell information security according to Harkins [22]. The same matter is discussed by Johnston *et al.* [17] under the term "fear appeal theory", which is a way of "scaring" others to behave in a specific way. Harkins [22] argues that relying on "fear" can have the opposite effect because people do not want to listen to negativity, with the effect that over time information security will lose credibility. Harkins [22] argues that we instead should focus on "solutions". From our understanding, focusing on solutions is the opposite of "fear appeal theory" and we define it as an "opportunistic approach" which is a way of proposing solutions to emphasise that information security is a business enabler.

We agree with Harkins [22] arguments that in general it is preferable to use the "opportunistic approach" as opposed to what Johnston *et al.* [17] calls "fear

appeal theory". However, we still think that both of these methods can be useful, depending on the situation, and a combination can help to illustrate both sides of the challenge with information security. Since people are different, the best method to use typically depends on the individual personal characteristics, which means that some prefer and understand rhetoric based on the "opportunistic approach" while other prefer the approach of the "fear appeal theory". The time frame can be a factor for deciding which approach to use. As an example, in situations of handling security incidents where decision-making must happen swiftly and where the focus is short term, it might be better to use "fear appeal theory". The "opportunistic approach" is probably better suited for negotiating business or strategic plans and long-term planning since it sets an optimistic tone while negotiating.

4.4 Pedagogy

Pedagogy is about how to structure BLIS in a manner that makes it easier to learn and teach efficiently. We argue that utilising BLIS needs dedication and combining many different fields, and is not as simple as speaking business language by using some business terms. A natural requirement for using business terms in communication with management is that the practitioner should have the foundational understanding of business concepts to discuss it critically. Simply focusing on learning terms but not having understanding could at worst result in a loss of credibility.

To develop BLIS and build a curriculum, it is important to have understanding of pedagogy, since it provides a basis for identifying appropriate teaching methods, and for constantly improving the program. Understanding pedagogy can also help the practitioners have a broader view and methods to teach others information security skills or build better culture.

Kolomiets & Konoplenko [2] suggest to use a "Business Game" which is a model based on "task-based learning". This was taught by simulating different situations that could occur in student´s later professional life to build their experience before graduating. This can also be beneficial for learning BLIS.

Drevin *et al.* [3] also suggest a linguistic approach to learning information security. This approach consists of developing a language around a topic, and measuring understanding with a vocabulary-measuring instrument in a group to test their knowledge and understanding of the language. This method is also applicable for learning BLIS since it consists of many different fields and is an excellent way to test the students and their understanding.

Based on the above discussion we see that BLIS is far too complex to be viewed just as "speaking" the business language, Hence, BLIS should be seen as a distinct field within information security, which should become a part of the "common body of knowledge" for information security practitioners and the next generations of students.

5 Future work

This paper proposes a theoretical framework for learning BLIS. The framework still needs to be validated for practicality, with its different components. The only way to understand another language is to learn it, and hence the next step should consist of letting a group of security professionals try it out in their working environment. The present study has focused on describing BLIS and benefits of learning it. We argue that students of information security need to learn how to communicate the importance that information security has for business, with the aim of obtaining management support and commitment. This paper describes a basis for developing a curriculum based on our proposed theoretical framework.

Our ongoing work will be to validate BLIS and improve the theoretical framework. We will interviewing CISOs to collect real business scenarios which will become learning material for the students, called "Security Business Games". Another activity will involve students who are attending continuing education and professional development by first presenting a business game without teaching BLIS, then to teach them BLIS followed by a similar, but different, business game. The aim will be to compare the data and conduct interviews on their experiences with BLIS. This represents a method to empirically validate BLIS and improve the BLIS curriculum.

Additionally, we will interview CISOs to gain more insight on what should be the core components and sub-components of BLIS, based on their experience from real business settings. This will allow us to compare data from interviews with the experience from applying BLIS in different business games, which provides empirical evidence to improve and validate the different components of BLIS. Each component and sub-component represents its own complex field that needs investigation to ensure that BLIS becomes practical and useful for information security professionals.

6 Conclusion

In this study, we have defined the BLIS and proposed a theoretical framework for learning it. We argue that BLIS is not for only communicating with management, but also a distinct field within information security. We argue that learning BLIS will help professionals and students with the practical use of information security in a business setting. The key components of BLIS are Business, Information Security, Communication, Soft Skills, and Pedagogy. These components are essential to learning and using BLIS in a business setting. We have elaborated to some extent on what these components consist of, which can be used to develop a curriculum to teach future students.

This research aims to gain better understanding and improve the business aspects of information security. The fundamental assumption is that information security is an essential business issue, and not just a technical issue. It is crucial to educate business leaders to understand this, and the purpose of BLIS is precisely to help security professionals in this endeavor. Generally, we believe that

BLIS is not just for communicating with management but is a way of integrating information security in business settings, and a way of defining information security as a core element of business management.

References

1. Ashenden, D., Sasse, A. CISOs and organisational culture: their own worst enemy?. *Computers & Security*. **39**, 396–405 (2013)
2. Kolomiets, S., Konoplenko, L. A model for teaching speaking English for Specific Purposes (information security) using business game. *Advanced Education*. **3**, 58–63 (2015)
3. Drevin, L., Kruger, H., Bell, A. & Steyn, T. A linguistic approach to information security awareness education in a healthcare environment. *IFIP World Conference On Information Security Education*, 87–97 (2017)
4. Alotaibi, Y. A Secure Business Process Modelling For Better Alignment between Business and IT. *2016 49th Hawaii International Conference On System Sciences (HICSS)*, 4793–4802 (2016)
5. Brucker, A. Integrating security aspects into business process models. *It–Information Technology*. **55**, 239–246 (2013)
6. Altuhhova, O., Matulevičius, R. & Ahmed, N. Towards definition of secure business processes. *International Conference On Advanced Information Systems Engineering*, 1–15 (2012)
7. Schinagl, S. & Paans, R. Communication barriers in the decision-making process: System Language and System Thinking. *Proceedings Of The 50th Hawaii International Conference On System Sciences*. (2017)
8. Abbass, W., Baina, A. & Bellafkih, M. Improvement of information system security risk management. *2016 4th IEEE International Colloquium On Information Science And Technology (CiSt)*, 182–187 (2016)
9. Sechi, F., Gran, B., Jørgensen, P., Kilyukh, O. Better Security Assessment Communication: Combining ISO 27002 Controls with UML Sequence Diagrams. *2022 IEEE/ACM 3rd International Workshop On Engineering And Cybersecurity Of Critical Systems (EnCyCriS)*, 49–56 (2022)
10. Moyón, F., Méndez, D., Beckers, K. & Klepper, S. Using Process Models to Understand Security Standards. *International Conference On Current Trends In Theory And Practice Of Informatics*, 458–471 (2021)
11. Rainer Jr, R., Marshall, T., Knapp, K. & Montgomery, G. Do information security professionals and business managers view information security issues differently?. *Information Systems Security*. **16**, 100–108 (2007)
12. Whitman, M. & Mattord, H. Information security governance for the non-security business executive. (2014)
13. Karanja, E. The role of the chief information security officer in the management of IT security. *Information & Computer Security*. (2017)
14. Jirasek, V. Practical application of information security models. *Information Security Technical Report*. **17**, 1–8 (2012)
15. Ashenden, D. Information Security management: A human challenge?. *Information Security Technical Report*. **13**, 195–201 (2008)
16. Soomro, Z., Shah, M. & Ahmed, J. Information security management needs more holistic approach: A literature review. *International Journal Of Information Management*. **36**, 215–225 (2016)

17. Johnston, A., Warkentin, M., Dennis, A. & Siponen, M. Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences*. **50**, 245–284 (2019)
18. AlGhamdi, S., Win, K., Vlahu-Gjorgievska, E. Information security governance challenges and critical success factors: Systematic review. *Computers & Security*. **99**, 102030 (2020)
19. Anu, V. Information security governance metrics: A survey and taxonomy. *Information Security Journal: A Global Perspective*. **31**, 466–478 (2022)
20. Fitzgerald, T. Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other. *Information Systems Security*. **16**, 257–263 (2007)
21. Whitten, D. The chief information security officer: An analysis of the skills required for success. *Journal Of Computer Information Systems*. **48**, 15–19 (2008)
22. Harkins, M. The 21st Century CISO. *Managing Risk And Information Security*, 139–153 (2016)
23. Hooper, V. & McKissack, J. The emerging role of the CISO. *Business Horizons*. **59**, 585–591 (2016)
24. Kayworth, T. & Whitten, D. Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*. **9**, 2012-52 (2010)
25. Posthumus, S. & Von Solms, R. A framework for the governance of information security. *Computers & Security*. **23**, 638–646 (2004)
26. Solms, S. & Solms, R. Information security governance. (Springer Science & Business Media,2008)
27. Mintzberg, H. Managerial work: Analysis from observation. *Management Science*. **18**, B97–B110 (1971)
28. Hersey, P., Blanchard, K. & Natemeyer, W. Situational leadership, perception, and the impact of power. *Group & Organization Studies*. **4**, 418–428 (1979)
29. Mills, J., Bonner, A. & Francis, K. The development of constructivist grounded theory. *International Journal Of Qualitative Methods*. **5**, 25–35 (2006)
30. Kitchenham, B. Procedures for performing systematic reviews. *Keele, UK, Keele University*. **33**, 1–26 (2004)
31. Tran, D. & Jøsang, A. Information Security Posture to Organize and Communicate the Information Security Governance Program. *Proceedings of the 18th European Conference On Management Leadership And Governance, ECMLG 2022*. **18**, 515–522 (2022)
32. Crang, M., Cook, I. & Others Doing ethnographies. (Sage,2007)
33. Glaser, B. Basics of grounded theory analysis: Emergence vs forcing. (Sociology press,1992)
34. Strauss, A. & Corbin, J. Basics of qualitative research techniques. (Citeseer,1998)
35. Standardization, I. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. (2022)
36. Helse, D. Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren. (2019)
37. Regjeringen Nasjonal strategi for digital sikkerhet. (2019)