Tools Supporting Information Security Risk Management in Practice

Erik Bergström[1,*,†]

[1]Department of Computer Science and Informatics, School of Engineering, Jönköping University, Jönköping, Sweden

Abstract

It is well-known that Information Security Risk Management (ISRM) activities can be challenging to perform and that tool support could provide support in different ways, for example, by automating tasks, guiding the user, or helping with documentation. Despite the need for tools, there is a lack of studies investigating ISRM tool usage. This paper contributes by presenting the results from one of the first studies targeting information classification and ISRM tool usage in practice. The study is based on a survey sent to government agencies in Sweden and was answered by 139 respondents (67%). The survey targeted the type of tools used and the perceptions of those tools. Findings include a list of tools perceived to contribute to performing ISRM activities, such as information classification, the reasons why the tools were selected, and how well they fulfil their needs. More specifically, we found that spreadsheets and document templates are the most common tools used – despite not being perceived as fulfilling the needs. We also found that taking on an even more holistic view might be needed when considering functionality in ISRM tools.

Keywords

Information classification, Information Security Risk Management, Tool support, Tools in practice

1. Introduction

Information assets are crucial to most organisations, and much effort and money are spent to secure them. Information Security Risk Management (ISRM) can be applied to do so in a structured way. There is a plethora of ISRM methods to choose from, and they can be quantitative, qualitative, or semi-quantitative [1] and have a different focus, e.g., on the public sector or small and medium-sized enterprises (SMEs) [2]. Regardless of the ISRM method, the goal is similar: to describe a continuous process to identify and mitigate risks toward critical information assets [3]. Before performing a risk analysis (RA), we need to know what assets exist in the organisation and how valuable they are. This activity is commonly referred to as information classification. As the result of the information classification serves as input to the RA [4, 5], the classification quality is critical and has been described as essential for the success of RA [6]. Despite being an important activity that is even compulsory for many organisations [5], information classification has been described as an understudied area [7, 8], especially the aspects of how information classification is practised in organisations [9, 10].

The 9th International Conference on Socio-Technical Perspectives in IS (STPIS'23) 27.-28.10. Portsmouth, UK

*Corresponding author.

erik.bergstrom@ju.se (E. Bergström)

0000-0002-1436-2980 (E. Bergström)

Tools can support the ISRM work in various ways, for example, by automating tasks [2], creating a more straightforward path between activities and reducing manual work that can generate errors [11]. Unfortunately, there is quite little literature on tool support for ISRM and its activities. Therefore, in this paper, we provide insights on tool usage in practice by investigating what tools are used to support the ISRM activity information classification and, in addition, the overall ISRM work in ISO/IEC 27001/27002-based organisations. The reason for focusing on tool support in such organisations is that no specific tools are provided with the standards and that the standards are mandated to be used by many organisations. Moreover, we investigate why the tools have been selected and how well the tools fulfilled the needs. In the literature, it is not evident to what extent there is a clear need for overall ISRM tool support and to what extent there is a need to support specific ISRM activities separately. Such understandings are important because we still lack insights into how organisations protect themselves in practice [12]. Therefore, we focus on both tool support for information classification and the overall ISRM work despite information classification being a part of ISRM.

This paper is organized as follows; the next section discusses ISRM and information classification and how tools support ISRM and the information classification activity. The following section introduces the study approach, followed by the results. The next section discusses the results, while the last section concludes the study.

2. Background

This section focuses primarily on ISRM and information classification and how tools can support the work.

2.1. ISRM and information classification

Several risk-based standards and methods exist that help organisations identify and value assets and select security controls to protect those assets [13]. Shameli-Sendi et al. [14] have identified over 30 such methods and standards published by professional organisations and researchers. Examples include the Central Computer and Telecommunications Agency Risk Analysis and Management Method (CRAMM), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), and NIST 800-30. It can be difficult for organisations to choose among the methods, and it is an important choice as it can affect the end result [15]. However, organisations might not have many alternatives in practice as they may be mandated to follow international standards, e.g., for getting government contracts [16]. Hence, for many organisations, there are only the ISO/IEC standards to choose from, and even if they use another standard, they might need to consider them to be compliant.

The differences between ISRM methods have been described as minor [17], and here we consider the general ISRM process to consist of the activities information classification, risk analysis, and the selection of security controls. After the selection of security controls, there is a feedback operation to the classification to review the classification and thereby continuously improve the controls. The exact tasks performed in the activities could differ, but what is covered in the process is similar [3].

In this work, we focus on information classification as it has not attracted as much attention as other ISRM activities [7], especially from a practice perspective [10]. Shedden et al. [8] concluded in their study that most ISRM methods were limited regarding asset management and classification, suggesting that less attention has been directed towards this topic compared to other ISRM activities. According to ISO/IEC 27002 [18], information classification has the purpose to *"ensure identification and understanding of protection needs of information in accordance with its importance to the organization"* [18, p.23]. The literature has identified several challenges related to information classification, including subjective judgement [19], what and how to document [10, 20], and what security aspects to consider [21, 22], all of which tool support could have the potential to alleviate.

2.2. ISRM and information classification tool support

It is not precisely clear what tool support implies in an ISRM context, and we have kept an inclusive approach to what it could be. A broad description of a tool is *"something that helps you to do a particular activity"* [23]. In an ISRM context, that implies tool support can be either a dedicated tool or something more rudimentary, such as spreadsheets, document templates or other supplementary support that helps the practitioner in their work [2, 15, 24]. There are few overviews of tools, but The European Union Agency for Cybersecurity (ENISA) maintains an inventory of over 30 Risk Management/Risk Assessment tools [25]. In addition, a recent report from ENISA [26] contains information on whether tool support is available as part of around 30 identified Risk Management methods. In addition, they present an additional eight tools that support risk management, but these tools are not evaluated or investigated in any detail. Common for the tools in the inventory is that they are developed to support specific standards and methods, and the activities performed are specified as a set of steps to follow [2], which implies that the activities are static rather than dynamic. There is some evidence in the literature that the activities are not as rational and sequential in practice [10, 27] and could, for example, be performed in parallel or in a different order [28]. Such aspects can contribute to limiting tool alternatives for organisations using the ISO/IEC 27000 family of standards as they do not provide a specific tool with the standards. This is perhaps extra troubling as we know that turning standards into practice is difficult [29, 30, 31]. A study by Bernsmed et al. [32] in the Air Traffic Management (ATM) domain confirms this situation. There, organisations use an adapted version of ISO/IEC 27005 [33] that is accompanied by additional documentation to fill the gaps in the standard [32] and a Microsoft Excel spreadsheet [34] was used as tool support by some of the investigated organisations. The spreadsheet users found several issues related to limited functionality, and among the organisations that did not use the spreadsheet, the lack of tool support was a significant issue [32].

Gritzalis et al. [2] have developed a method for selecting an appropriate risk assessment method based on criteria and also compared ten popular methods in their study. In their comparison, tool support is considered, and most investigated methods support or contain tools. They describe simpler tools such as spreadsheets as providing limited functionality and being restrictive and disadvantageous compared to dedicated software. However, even the more advanced tools had drawbacks, such as predefined tables for information classification and input limitations regarding what can be entered during documentation [2].

Literature also mentions other issues with both standards and tools; that they generally fail to answer fundamental questions regarding tasks performed in ISRM activities, for example, how to separate critical and non-critical resources and how to calculate the likelihood of a threat [14], and the order to perform tasks [15].

There is very little literature on tool support for information classification [35], regardless if the perspective is a dedicated tool for classification or if the classification functionality is included in a more encompassing ISRM tool. Asaf et al. [36] identified eight tools for automatic document classification, which could be seen as a subset of information classification in their study. All of the identified tools had limitations. Also worth mentioning is that the focus of such tools is the classification of individual documents (i.e. a high granularity approach) rather than the classification of processes or systems, which is the standard approach in classification [10]. There is also a study [37] on using one classification tool, but this study focuses on stress among novice ISRM practitioners. Nonetheless, are there some interesting findings from a tool perspective. Tools were perceived as helpful because the tool provided suggestions on security controls. There were also some issues. There were problems with the flexibility of the tool, e.g. when workflow and terminology in the tool differed from organisational practice and with the documentation of the classification.

3. Method

In order to capture tool usage and the perception of using the tools, a survey was selected as the method. The survey was constructed in two parts, one part focusing on the information classification activity and one part focusing on the overall ISRM work. Each part had a set of questions targeting both quantitative and qualitative data. We wanted to find out what tools are used for supporting the information classification and overall ISRM work and how common those respective tools are. Because the study is explorative and we knew beforehand that respondents could interpret what a tool is differently, we clarified the questions by explicitly mentioning that, for example, spreadsheets count as tool support. We did, however, not mention any specific product to lead the respondents. In addition, did we also want to investigate the perception of those tools, i.e., why the tools were selected and how well they fulfilled their needs. Finally, if no tools were used in their classification or ISRM work, we asked why they chose not to use any.

It is well-known that it is a hard challenge to collect data in the information security field [12, 38]. To get a high response rate, we undertook several measures. Firstly (1), we targeted Swedish public sector organisations, and since they fall under the principle of public access to official records, the internal policies and practices are more accessible than in private organisations. In addition is there a regulation [39] that demands the public sector to work systematically and risk-based and to follow the ISO/IEC 27001 [40] and ISO/IEC 27002 [18] standards. However, there is no required practice in implementing or using them, leading to a situation where the public sector has adopted different practices based on the ISO/IEC standards [10]. Secondly (2), we sent the survey as plain text in an email and asked them to answer by replying to the email rather than using any of the established online survey tools. Such an approach creates extra work, but we believe many CISOs would not click on links, especially since they probably tell colleagues about phishing risks. Lastly (3), we used reminders for an extended period. The first request was sent out in the spring of 2022, and the last data was collected at the beginning of 2023.

All answers from the survey were collected in a large spreadsheet, and the statistics on tool usage supporting information classification (see results in 4.1.1) and ISRM (see 4.2.1) were put together. In order to get a better understanding of the tools, all collected tools were investigated by visiting the respective software developer's web page. The free-text answers were separated per question and divided into groups based on whether or not Microsoft Excel was used as a tool. The questions on the reasons for selecting the tools (see 4.1.2 for information classification tools and 4.2.2 for ISRM tools) were thematically analysed [41], and the coding revealed eight categories. For the question of how well the classification tool fulfils their needs (see 4.1.3), all answers were divided into three groups (not acceptable, marginal and acceptable) inspired by the system usability scale (SUS) [42]. Finally, the survey was constructed so that if the respondents did not use any tool to support their classification or ISRM work, they could explain why they had chosen not to. Four themes emerged after a thematic analysis [41] of the responses (see 4.3).

4. Results

The survey was sent to 255 governmental agencies. Out of those, 48 were excluded as they lacked their own administration (most had zero employees), or their information security work was performed through another agency, leaving the group in focus at 207 agencies. Out of those, 139 answered the survey (67%).

The result section is divided into three parts: tools supporting information classification, tools supporting the overall ISRM work, and finally, one section on why organisations had chosen not to use tool support.

4.1. Information classification tool support

This section presents an overview of the tool support for information classification.

4.1.1. What tools supporting information classification are used?

As can be seen in Table 1, the survey revealed the usage of 18 tools supporting classification. Microsoft Excel is the most common tool, and Microsoft Word is the second most used. Twenty-six organisations used a combination of tools, i.e., several tools were mentioned in their response, such as spreadsheets combined with a document management system.

Based on the description of the respective tools' websites, we can see that most of the tools are not specifically developed for the information classification activity. Of the 18 different tools, only four were related to information classification. Apart from the traditional office suite tools, two main categories of tools were mentioned: tools that support process management and document management tools.

Table 1
Overview of the tools used to support information classification. The type of tool column describes how the developer describes the tool.

Developer - Tool	Users	Link to the web page of the tool/note	Type of tool
Microsoft – Excel	75	https://www.microsoft.com	Spreadsheet
Microsoft – Word	26	https://www.microsoft.com	Word processor
VisAlfa – VisAlfa	8	https://www.visalfa.se	Process-based information identification and management
The Swedish Civil Contingencies Agency - Infosäkkollen [Infosec check]	4	https://www.msb.se/infosakkollen	Follow-up and comparison with other similar organisations (related to baselining)
Atlassian – Confluence	2	https://www.atlassian.com	Wiki (knowledge management, collaboration)
Microsoft – Sharepoint	2	https://www.microsoft.com	Content management system
Omegapoint – Ciso	2	https://ciso.se	ISMS support
2c8 – 2c8 Apps	1	https://www.2c8.com	Process mapping and modelling
Addsystems – ADD	1	https://www.addsystems.com	Management system support (e.g., document, case and process management)
Own development	1	One agency has developed its own tool	Case management and registration
Formpipe Software – Platina	1	https://www.formpipe.com	Document management system and registration
Ida Infront - iipax case	1	https://idainfront.se	Case management and archiving
Microsoft – PowerPoint	1	https://www.microsoft.com	Presentation
Microsoft – Visio	1	https://www.microsoft.com	Diagramming
OpenText – Documentum D2	1	https://www.opentext.com	Enterprise content management
Software AG – ARIS Enterprise	1	https://www.softwareag.com	Enterprise management system
Stratsys – GRC management	1	https://www.stratsys.com	GRC (Governance, Risk management, and Compliance) management
Swedish Association of Local Authorities and Regions – Klassa [Classify]	1	https://klassa-info.skr.se	Information classification and GAP analysis

4.1.2. Why were the information classification tools selected?

Seventy-five respondents answered the survey question on why they selected their classification tool. Following a thematic analysis, eight themes emerged, as seen in Table 2.

The most common reason had to do with user-friendliness or ease of use. A common argument among Microsoft Excel users was that it has a familiar interface that most recognize and can

Table 2
Overview of why the tools used to support information classification were selected.

Reasons	Count
User-friendly/easy to use	25
Readily available/format	13
Good enough	11
No viable alternatives	10
Inheritance/recommendation	8
Coherent/structured	7
Flexible/adaptable	7
Inexpensive	2

use. The second most mentioned reason (all by Microsoft Excel users) was that the tool was available for most users. Several in this group also mentioned that it was a file format that was accessible to many. Next came a group of users claiming they selected the tool because it was good enough. It helped them to solve the task. Eight organisations either inherited their tool or got a recommendation (from consultants or colleagues in other organisations) to use it. One group selected the tool because it provided structure and contributed to a more coherent ISMS process. In this group, only two used spreadsheets. Finally, one group chose their tool because of the flexibility to adapt the structure and content in spreadsheets, and one group referred to the low cost of using an already installed tool.

4.1.3. How well do the information classification tools fulfil their needs?

One free-text question was asked to investigate how well the classification tool fulfils their needs. Sixty-five answers were given, and in the analysis, we divided the responses into three groups (not acceptable, marginal, and acceptable) based on a scale inspired by SUS (Brooke, 1996). An overview of the result can be seen in Fig. 1.

The not acceptable group (examples of adjectives used: bad, poor, not well) (n=23) contained many reasons why their tool did not fulfil their needs. Common causes of why the tool support was not perceived as fulfilling their needs included that it was not easy to use, not mature enough, lacked a central repository for classified assets, and was not created for classification. Some also reflected that the tool didn't support the classification itself or, as they put it: *"The support works well for documenting the classification, but not for the classification activity."*

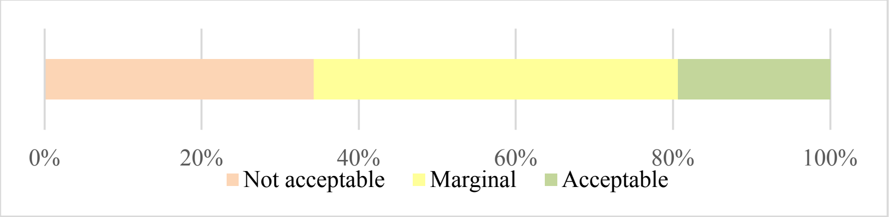

Figure 1: An overview of how the respondents perceive the tool to fulfil their needs.

The marginal group (examples of adjectives used: ok, well enough, satisfactory) was the largest (n=31) and a relatively homogenous group. Several respondents reflected that the tool was satisfactory, but they would prefer even more support. The Microsoft Excel users mainly reflected that the tool was not developed specifically to support classification. Also, mentions of having tools supporting more activities than just the classification decreased the tool perception.

The acceptable group (examples of adjectives used: good, excellent, very well) (n=13) was the smallest group and the group that provided the shortest answers. The few reasons given included the possibilities to adapt the tool.

4.2. ISRM tool support

This section presents an overview of tool support for the overall ISRM work.

4.2.1. What tools supporting ISRM are used?

Table 3 presents an overview of 14 tools mentioned to support the overall ISRM work. Fifteen organisations said they used a combination of two or more tools to support their ISRM. Similarly to information classification, Microsoft Excel, followed by Microsoft Word, was the most common tool support. As with information classification support, the risk analysis activity was mentioned to be based on spreadsheet-based templates. Six of the tools are specifically information security-related software.

4.2.2. Why were the ISRM tools selected?

Forty-nine respondents answered the survey question on why they selected their classification tool. The eight themes identified for classification tools were used to classify the results for ISRM tools. Table 4 shows an overview of the results.

Similarly to the classification tool support analysis, user-friendliness is the main reason for the tool selection. The other two top three reasons were that the tool was readily available for most or all users and good enough for the activities.

4.3. Why are some organisations not using tools to support information classification or ISRM?

In total, 43 free-text answers were given to this question. Four themes emerged during the thematic analysis of the responses. The most common reason (16 answers) for not using any tool support was that the organisation had not started classifying their information or systematically started their ISRM work yet. A typical response was: *"unfortunately, we are far behind with the information classification work largely due to a lack of resources. We have had problems recruiting staff."* Ten respondents felt manual work was sufficient and did not need tool support. Eight respondents answered that they wanted to use a tool but could not find one that fulfilled their requirements. The reasons for this varied, but six lacked a tool that supported and incorporated the entire information security management system with its associated activities. Two of the respondents were in the process of developing their own tool support, and five respondents could not give a reason.

Table 3
Overview of the tools used to support the overall ISRM work. The type of tool column describes how the developer describes the tool.

Developer - Tool	Users	Link to the web page of the tool	Type of tool
Microsoft – Excel	47	https://www.microsoft.com	Spreadsheet
Microsoft – Word	16	https://www.microsoft.com	Word processor
The Swedish Civil Contingencies Agency–Infosäkkollen [Infosec check]	5	https://www.msb.se/infosakkollen	Follow-up and comparison with other similar organisations (related to baselining).
Stratsys – GRC Management	4	https://www.stratsys.com	GRC management
2c8 – 2c8 Apps	1	https://www.2c8.com	Process mapping and modelling
Addsystems – ADD	1	https://www.addsystems.com	Management system support (e.g., document, case and process management)
Atlassian – Confluence	1	https://www.atlassian.com	Wiki (knowledge management, collaboration)
iFACTS	1	https://www.ifacts.se	GRC management
Microsoft – Sharepoint	1	https://www.microsoft.com	Content management system
Microsoft – Visio	1	https://www.microsoft.com	Diagramming
Omegapoint – Ciso	1	https://ciso.se	ISMS support
Mural – Mural	1	https://www.mural.co	Digital whiteboard (visualization of processes, workflow, mindmaps)
Swedish Association of Local Authorities and Regions – Klassa [Classify]	1	https://klassa-info.skr.se	Information classification and GAP analysis
Visma Draftit – Draftit DPIA	1	https://www.visma.se	Data Protection Impact Assessment

Table 4
Overview of why the tools used to support the overall ISRM work were selected.

Reasons	Count
User-friendly/easy to use	16
Good enough	12
Readily available/format	9
Coherent/structured	6
No viable alternatives	5
Flexible/adaptable	3
Inheritance/recommendation	2
Inexpensive	1

5. Discussion

The results have several interesting findings regarding the tools used to support classification and ISRM. First and foremost, Microsoft Excel was found to be the most well-used tool. It is unsurprising as Microsoft Office-based templates are available at a national site [27], giving practical advice for working systematically with information security. The intention is to help turn standards into practice, which has been described as extra difficult for information classification [43]. The fact that Microsoft Office is the dominant software in most countries and the file formats are possible to use in other office software makes it a natural choice for distributing templates.

When looking at the most common reasons why the tools were selected, most respondents stated that they picked them because they were user-friendly, easy to use, readily available, and good enough. All these reasons indicate a positive experience that at least gets the job done. On the other hand, when we questioned how well the tool fulfils their needs, less than 20% used positive adjectives such as good and excellent. In addition, a large group uses their tool because there are no viable alternatives, and some non-tool users do manual work because they do not find a tool that supports them. These results suggest that there is indeed a need for tools, but the tools used do not deliver what is needed from an organisational perspective for most users. The reasons for this could include limitations in the available tools.

Several tools were neither dedicated ISRM tools nor office suite tools, and those tools helped organisations in other ways. Based on the type of tools mentioned and responses in the free-text questions, it is possible to point towards some needs. There is a need to support the whole life cycle of information classification and ISRM. The input to information classification is often a process, and if the process mapping/modelling and process management are in another tool, that tool also supports the classification. That could explain the usage of process management software. Similarly, after a classification, you will have a filled spreadsheet or another document containing documentation that must be stored somewhere. Hence, respondents mentioning case management systems, document management systems, and archiving software point towards a documentation support need. To have a broader lifecycle perspective for classification is not a new belief [9], but how it is enacted in practice is still not evident. For ISRM tools, the situation is similar, but a few more references to dedicated ISRM software were found among the responses.

6. Conclusions

This study is one of the first studies presenting an overview of what tools are used to support information classification and the overall ISRM work in practice. This paper shows that most investigated organisations use Microsoft Office products to support their classification or other ISRM activities. The rest of the tools used are a mix of dedicated ISRM tools and other tools. A number of reasons for tool selection were found, but at the same time, we could conclude that, in general, the users perceived the tools did not fulfil their needs. We recommend that future studies focus more on the underlying reasons, perhaps using interviews or another approach that could shed more light on the underlying motivations for ISRM tool selection. We have also seen a need to narrow down the requirements for tools supporting ISRM and its activities, such as information classification. This is especially important since we investigated the need among organisations using the ISO/IEC standards that come without dedicated tool support or specific tool recommendations.

It would also be interesting to investigate why many organisations perceive that there are no viable tool alternatives to support their ISRM. Are there tool requirements that make some of the existing tools impossible to use in the public sector? Is it a communication issue or something else? One can also reflect on the situation where spreadsheets of document templates are given as examples, e.g., as described previously in the example from the ATM domain or as seen in this study. If templates are given, do the organisations perceive them as an example, or do they believe they provide enough support to complete the task rather than exemplify it? There is an obvious risk that the availability of templates and rudimentary tools that rather exemplify functionality is seen as a full-fledged tool that inhibits the use of dedicated ISRM tools. Here, we cannot provide any definitive answer, and future studies are suggested, especially as spreadsheets are used in other domains as support for turning standards into practice or for providing tool support.

Finally, it is evident that there is a need to not see the activities in ISRM as isolated activities that individually need tool support, but rather a holistic approach with a more encompassing tool would be preferred. Exactly where the limitations should be drawn is unclear from this study, and it is suggested for future researchers to help identify. However, this study indicates that tools should support process management and document management, i.e., a bit wider view than the traditional lifecycle view.

Acknowledgments

We gratefully acknowledge the grant from the Swedish Civil Contingencies Agency (MSB), project VISKA (MSB 2021–14650).

References

[1] M. Alohali, A Model for User-centric Information Security Risk Assessment and Response, Ph.D. thesis, University of Plymouth, Plymouth, UK, 2019.

[2] D. Gritzalis, G. Iseppi, A. Mylonas, V. Stavrou, Exiting the risk assessment maze: A meta-survey, ACM Comput. Surv. 51 (2018) 1–30. doi:10.1145/3145905.

[3] E. Bergström, M. Lundgren, A. Ericson, Revisiting information security risk management challenges: A practice perspective, Information and Computer Security 27 (2019) 358–372. doi:https://doi.org/10.1108/ICS-09-2018-0106.

[4] F. Karlsson, P. J. Ågerfalk, Towards structured flexibility in information systems development: Devising a method for method configuration, Journal of Database Management (JDM) 20 (2009) 51–75. URL: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/jdm.2009070103. doi:10.4018/jdm.2009070103.

[5] S. Ozkan, B. Karabacak, Collaborative risk method for information security management practices: A case context within turkey, International Journal of Information

Management 30 (2010) 567–572. URL: http://www.sciencedirect.com/science/article/pii/S0268401210001222. doi:http://dx.doi.org/10.1016/j.ijinfomgt.2010.08.007.

[6] C. Everett, Building solid foundations: the case for data classification, Computer Fraud Security 2011 (2011) 5–8. URL: http://www.sciencedirect.com/science/article/pii/S1361372311700604. doi:http://dx.doi.org/10.1016/S1361-3723(11)70060-4.

[7] J.-H. Bergquist, S. Tinet, S. Gao, An information classification model for public sector organizations in sweden: a case study of a swedish municipality, Information Computer Security 30 (2021) 153–172. URL: https://doi.org/10.1108/ICS-03-2021-0032. doi:10.1108/ICS-03-2021-0032.

[8] P. Shedden, A. Ahmad, W. Smith, H. Tscherning, R. Scheepers, Asset identification in information security risk assessment: A business practice approach, Communications of the Association for Information Systems 39 (2016) 15.

[9] E. Bergström, R.-M. Åhlfeldt, Information Classification Issues, Lecture Notes in Computer Science, Springer International Publishing, 2014, pp. 27–41. URL: http://dx.doi.org/10.1007/978-3-319-11599-3_2. doi:10.1007/978-3-319-11599-3_2.

[10] E. Bergström, Supporting Information Security Management: Developing a Method for Information Classification, Ph.D. thesis, University of Skövde, Skövde, Sweden, 2020.

[11] E. Bergström, M. Lundgren, K. Bernsmed, G. Bour, "check, check, check, we got those" – catalogue use in information security risk management, in: S. Furnell, N. Clarke (Eds.), Human Aspects of Information Security and Assurance, Springer Nature Switzerland, ????, pp. 181–191. doi:https://doi.org/10.1007/978-3-031-38530-8_15.

[12] R. Baskerville, F. Rowe, F.-C. Wolff, Integration of information systems and cybersecurity countermeasures: An exposure to risk perspective, SIGMIS Database 49 (2018) 33–52. doi:10.1145/3184444.3184448.

[13] R. Baskerville, P. Spagnoletti, J. Kim, Incident-centered information security: Managing a strategic balance between prevention and response, Information Management 51 (2014) 138–151. URL: http://www.sciencedirect.com/science/article/pii/S0378720613001171. doi:https://doi.org/10.1016/j.im.2013.11.004.

[14] A. Shameli-Sendi, R. Aghababaei-Barzegar, M. Cheriet, Taxonomy of information security risk assessment (isra), Computers Security 57 (2016) 14–30. URL: http://www.sciencedirect.com/science/article/pii/S0167404815001650. doi:https://doi.org/10.1016/j.cose.2015.11.001.

[15] G. Wangen, Information security risk assessment: A method comparison, Computer 50 (2017) 52–61. doi:10.1109/mc.2017.107.

[16] A. Gillies, Improving the quality of information security management systems with iso27000, The TQM Journal 23 (2011) 367–376. URL: http://www.emeraldinsight.com/doi/abs/10.1108/17542731111139455. doi:doi:10.1108/17542731111139455.

[17] S. Fenz, J. Heurix, T. Neubauer, F. Pechstein, Current challenges in information security risk management, Information Management Computer Security 22 (2014) 410–430. URL: https://www.emeraldinsight.com/doi/abs/10.1108/IMCS-07-2013-0053. doi:doi:10.1108/IMCS-07-2013-0053.

[18] ISO/IEC 27002, Information security, cybersecurity and privacy protection — Information security controls, Standard ISO/IEC 27002:2022, International Organization for Standardization, Geneva, CH, 2022. URL: https://www.iso.org/standard/75652.html.

[19] M. L. Kaarst-Brown, E. D. Thompson, Cracks in the security foundation: Employee judgments about information sensitivity, in: Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, ACM, 2009, pp. 145–151. doi:10.1145/2751957.2751977.

[20] M. R. Grimaila, L. W. Fortson, Towards an information asset-based defensive cyber damage assessment process, in: 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications, 2007, pp. 206–212. doi:10.1109/CISDA.2007.368155.

[21] O. Na, L. W. Park, H. Yu, Y. Kim, H. Chang, The rating model of corporate information for economic security activities, Security Journal 32 (2019) 435–456. URL: https://doi.org/10.1057/s41284-019-00171-z. doi:10.1057/s41284-019-00171-z.

[22] M. E. Whitman, H. J. Mattord, Principles of Information Security, fifth ed., Cengage Learning, 2014.

[23] Cambridge University Press Assessment, TOOL | English meaning - Cambridge Dictionary, 2023. URL: https://dictionary.cambridge.org/dictionary/english/tool.

[24] G. Wangen, C. Hallstensen, E. Snekkenes, A framework for estimating information security risk assessment method completeness, International Journal of Information Security 17 (2018) 681–699. URL: https://doi.org/10.1007/s10207-017-0382-0. doi:10.1007/s10207-017-0382-0.

[25] European Union Agency for Cybersecurity (ENISA), RM/RA Tools, 2023. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools.

[26] C. Lambrinoudakis, S. Gritzalis, C. Xenakis, S. Katsikas, M. Karyda, A. Tsochou, K. Papadatos, K. Rantos, Y. Pavlosoglou, S. Gasparinatos, A. Pantazis, A. Zacharis, Compendium of Risk Management Frameworks with Potential Interoperability: Supplement to the Interoperable EU Risk Management Framework Report, Report, European Union Agency for Cybersecurity (ENISA), 2022. URL: https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks.

[27] L. Coles-Kemp, Information security management: An entangled research challenge, Information Security Technical Report 14 (2009) 181–185. URL: http://www.sciencedirect.com/science/article/pii/S1363412710000063. doi:http://dx.doi.org/10.1016/j.istr.2010.04.005.

[28] D. B. Parker, Comparison of risk-based and diligence-based idealized security reviews, EDPACS 36 (2007) 1–12. URL: https://doi.org/10.1080/07366980701804805. doi:10.1080/07366980701804805.

[29] K. Njenga, I. Brown, Conceptualising improvisation in information systems security, European Journal of Information Systems 21 (2012) 592–607. URL: https://doi.org/10.1057/ejis.2012.3. doi:10.1057/ejis.2012.3.

[30] P. Shedden, W. Smith, A. Ahmad, Information security risk assessment: towards a business practice perspective, in: Proceedings of the 8th Australian Information Security Management Conference, School of Computer and Information Science, Edith Cowan University, Perth, 2010, pp. 119–130. doi:10.4225/75/57b6769334787.

[31] R. G. Taylor, J. Brice, Jeff, Fact or fiction? a study of managerial perceptions applied to an analysis of organizational security risk, Journal of Organizational Culture, Communications and Conflict 16 (2012). URL: https://www.proquest.com/docview/1037691839.

[32] K. Bernsmed, G. Bour, M. Lundgren, E. Bergström, An evaluation of practitioners' perceptions of a security risk assessment methodology in air traffic management projects, Journal of Air Transport Management 102 (2022) 102223. URL: https://www.sciencedirect.com/science/article/pii/S0969699722000448. doi:10.1016/j.jairtraman.2022.102223.

[33] ISO/IEC 27005, Information security, cybersecurity and privacy protection — Guidance on managing information security risks, Standard ISO/IEC 27005:2022, International Organization for Standardization, Geneva, CH, 2022. URL: https://www.iso.org/standard/80585.html.

[34] K. Labunets, Security Risk Assessment Methods: An Evaluation Framework and Theoretical Model of the Criteria Behind Methods Success, Ph.D. thesis, University of Trento, Trento, Italy, 2016.

[35] J. Breier, Asset valuation method for dependent entities, Journal of Internet Services and Information Security (JISIS) 4 (2014) 72–81. doi:10.22667/JISIS.2014.08.31.072.

[36] S. Asaf, D. Cohen, M. Moffie, M. Barham, European Security in Health Data Exchange, Deliverable D5.2, Data Sensitivity Analysis Tool, Report, 2017. URL: https://project-shield.eu/Content/PDFs/D5.2.pdf.

[37] E. Bergström, M. Lundgren, Stress amongst novice information security risk management practitioners, Intl. Journal on Cyber Situational Awareness 4 (2019) 128–154. URL: https://c-mric.com/100128. doi:10.22619/IJCSA.2019.100128.

[38] W. A. Cram, J. D'Arcy, J. G. Proudfoot, Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance, MIS Quarterly 43 (2019) 525–554. doi:10.25300/MISQ/2019/15117.

[39] MSBFS 2020:6, Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter [The Swedish Civil Contingencies Agency's Regulations on Government Agencies Security Information Security], Report, Myndigheten för samhällsskydd och beredskaps författningssamling, 2020. URL: https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-6-foreskrifter-om-informationssakerhet-for-statliga-myndigheter.pdf.

[40] ISO/IEC 27001, Information technology – Cybersecurity and privacy protection – Information security management systems – Requirements, Standard ISO/IEC 27001:2022, International Organization for Standardization, Geneva, CH, 2022. URL: https://www.iso.org/standard/27001.

[41] L. Ayres, Thematic coding and analysis, The Sage encyclopedia of qualitative research methods (2008) 868–869. URL: http://srmo.sagepub.com/view/sage-encyc-qualitative-research-methods/n451.xml.

[42] J. Brooke, Sus-a quick and dirty usability scale, in: P. W. Jordan, B. Thomas, I. L. McClelland, B. Weerdmeester (Eds.), Usability Evaluation In Industry, 1st edition ed., CRC Press, London, 1996. URL: https://doi.org/10.1201/9781498710411. doi:10.1201/9781498710411.

[43] E. Niemimaa, M. Niemimaa, Information systems security policy implementation in practice: from best practices to situated practices, European Journal of Information Systems 26 (2017) 1–20. URL: http://dx.doi.org/10.1057/s41303-016-0025-y. doi:10.1057/s41303-016-0025-y.