





Information Technology Consulting Firms' Readiness for Managing Information Security Incidents

Christine Große^(✉) , Maja Nyman, and Leif Sundberg 

Mid Sweden University, 851 70 Sundsvall, Sweden
{christine.grosse,leif.sundberg}@miun.se,
many1307@student.miun.se

Abstract. Because of the increase in the number and scope of information security incidents, proper management has recently gained importance for public and private organizations. Further challenges in this area have resulted from new regulations, such as the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS), as well as a tendency to outsource vital services to subcontractors. This study addresses the lack of empirical studies in the field and focuses on information security incident management at information technology (IT) consulting firms. Specifically, it examines challenges due to their exposed position and new regulations. The contribution of the paper is twofold. First, it provides valuable insight into the experiences and challenges of Swedish IT consulting firms. Second, it proposes criteria for classifying an information security incident that can equip decision-makers with a solid and assessable basis for incident management. The results emphasize further improvements in employee awareness, incident classification, and systemic governance, thereby integrating corporate policy making, information security incident management, and information system leadership.

Keywords: Security awareness · Information security incident management · Systemic governance · Incident classification · GDPR · NIS directive

1 Introduction

Recent violations of information security (InfoSec) in Sweden have included leaks of the healthcare hotline 1177 [1] and the Swedish Transport Agency [2, 3] as well as the access of unauthorized persons to the Swedish power grid [4]. The majority of these violations relate to the outsourcing of vital information technology (IT) services and inadequate handling of data by subcontractors. Therefore, the increase in outsourcing and the globalization of service providers have contributed to a growing number of incidents concerning InfoSec. In this context, an incident refers to an event that has the potential to impair the security of information in an unexpected or unwanted manner. Negative consequences pose threats to an organization that might disrupt productivity and lead to economic losses, legal implications, damaged image, and diminished trust among business partners and customers [5]. The risk of becoming the target of an

attack is rising alongside the value and sensitivity of the information that organizations and their subcontractors handle [6–8]. This field of tensions has produced a complicated situation wherein IT consulting firms must confront particular challenges in information security incident management (ISIM) due to their vulnerable position as subcontractors. However, a structured ISIM contains not only operational incident management but also awareness training for employees, mitigation of identified vulnerabilities, and analysis and preparedness activities [6, 9]. Although several standards and guidelines for ISIM have been developed, they have received criticism for their generality, which is a barrier to implementation for organizations [10].

Since subcontractors have access to the data of several customers, they are at higher risk of becoming targets of cyber attacks [11]. However, there is still a substantial lack of research on ISIM at consulting firms in general and IT consulting firms in particular [7]. The few studies that have investigated the implementation and operation of ISIM in practice at public or private organizations have advocated for more specific guidance for organizations and further empirical investigations [12]. Therefore, the present study seeks to address the considerable need for empirical research and a concentration on ISIM in IT consulting firms. It specifically explores challenges that relate to both the subcontractor position of firms and the occurrence of new regulations, such as the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS) in 2018. These relatively new regulations reflect significant developments in the fields of InfoSec, data protection, and critical infrastructure protection over the past two decades. Nevertheless, they have also created deep uncertainty among organizations with regard to how to comply with the requirements [13], and they remain poorly understood, as evident from the examples above and the following results of this study. In Sweden, the requirement to report incidents has led to a variety of reporting channels to numerous supervision authorities. Moreover, it has prompted delays ranging from over a week to a month [14, 15].

This paper builds on our previous research [16] by providing further novel content that broadens and enriches knowledge of ISIM in IT consulting firms. The study extends the representation of the interviews with critical quotations from participants. Furthermore, it adds analysis of the survey material and surpasses the scope of the previous research by proposing a model for the classification of InfoSec incidents. The research question of this study is, “which challenges do IT consulting firms encounter with respect to their ISIM, and how can these experiences inform future developments and inter-organizational learning?” The contribution of this paper is twofold. First, it identifies the challenges on the basis of interviews at three Swedish IT consulting firms with more than 20 employees. This information extends and clarifies the body of knowledge with specific insights regarding ISIM in practice. Second, the findings underpin the creation of a conceptual model for the classification of InfoSec incidents. Thus, they provide novel knowledge to enhance future developments of ISIM in theory and practice.

Following this introduction, the paper explains the background and methods of the study. Subsequently, it incorporates experiences of the IT consulting firms to highlight several challenges of ISIM and inform the incident classification model. The study concludes with a discussion of the implications for theory and practice as well as suggestions for further research.

2 Background

2.1 Foundations of InfoSec

InfoSec concerns the preservation of three qualities with regard to data and information: confidentiality, integrity, and availability [17]. The management of InfoSec needs to balance these cornerstones to support daily business operations and avoid interfering with the necessary information flow. However, recent technological developments and the increasing interconnectedness of society have imparted additional complexity to the management of InfoSec. These trends are already underway and continue to dissolve the boundaries of the classical computer system. Thus, the modern information system extends beyond technical artifacts to encompass formal and informal information flows within and between organizations in addition to the technical information transmission paths [18]. Moreover, the modern information system contains increasingly diverse customers. Therefore, InfoSec must address the protection of customers' personal information. The privacy of individuals is emerging as the fourth pillar in InfoSec primarily because of the GDPR, which has applied to the European Union (EU) since May 25, 2018 [11, 19]. The GDPR targets the protection of individuals and the information about them that organizations process. The regulation seeks to unify requirements regarding privacy within the EU and reflect the changed prerequisites of digitalization in society. Since the GDPR focuses on individual rights, it is also applicable outside of the EU if the processed information concerns a citizen of an EU Member State [20]. Organizations must consider the following requirements:

- Establishment of data portability and transparency
- Limitation of data collection and storage to specified purposes
- Assessment of consequences with regard to data breaches
- Appointment of a data protection officer
- Reporting of incidents regarding personal data within 72 h
- Responsibility for processed data and information
- Ability to demonstrate compliance with InfoSec in general and GDPR in particular
- Training of personnel that have access to personal data and information.

The regulation further criminalizes any failure to comply with the requirements and suggests costly penalties for organizations that are in breach of the regulation. Therefore, the content of incident reports must include not only facts about the type, magnitude, and effects of the incident but also details of how the incident has been threatened, which delimits the negative consequences of the security breach [11]. Thus, the responsible national authority can not only assess compliance to regulations but also inform other organizations and customers about breaches and mitigation activities.

Another regulation, the NIS, has the objective of protecting society from failures in InfoSec that can severely disturb important societal services, such as critical infrastructure. The NIS has applied since May 10, 2018 [21]. It targets providers of critical infrastructure, such as digital, finance, and health services, energy, water, and food supplies, and transportation. In contrast to the GDPR, the NIS aims to advance InfoSec in the context of critical infrastructure protection within the EU Member States. Concerned organizations must identify themselves as providers or operators of critical

infrastructure and establish measures for the prevention and mitigation of incidents in information systems and networks, which also includes planning for the swift restoration of the societal functionality. To meet the requirements of the recent regulations, an adequate ISIM must complement the systematic InfoSec management, which is now a precondition for public and private organizations. In extension of the GDPR, the NIS more strictly requires providers of critical infrastructure to contend with risks and practice risk-based ISIM. Incidents that are judged to yield serious consequences for the maintenance of critical infrastructure or digital services should be reported to the supervising agency as quickly as possible. The requirements for reporting are similar to those in the GDPR, especially the 72-hour maximum timeline for reporting an incident. In Sweden, the supervision agency recently divided this requirement into three steps of reporting: an initial announcement of the incident within six hours, a concretizing follow-up within 24 h, and a detailed follow-up within four weeks with the possibility of completing the report within one year [22]. Non-compliance can also be subject to penalties; however, in contrast to the GDPR, they are more moderate and depend on the level of non-fulfillment. Meanwhile, the demand for reporting incidents similarly concerns those that occur among subcontractors, such as IT consulting firms. In addition to the reporting requirements of the GDPR, the NIS demands information about both types of measures: those that prevent the incident's spread and reoccurrence as well as those that improve the ISIM at the reporting organization [21].

2.2 Framework for ISIM

Several best practices and guidelines are associated with ISIM, including the international standards ISO/IEC 27035:2016 and NIST SP 800-61 (Rev 2) (hereafter referred to as ISO and NIST, respectively) [8, 23]. Moreover, practical guides are regularly published by, for example, the SANS Institute, CERT Coordination Centre, and ENISA, which are based on the ISO and NIST standards. Gaps between the standards and the new regulations have been identified and encourage further alignment, particularly with regard to privacy [19].

In general, the process of a structured ISIM contains several phases. Specifically, ISO suggests five, while NIST dictates four phases for structuring the strategic and operative work that relates to incidents. Both standards provide organizations with generic principles and content [24] to permit applicability to any type of organization in regard to, for example, operation systems, applications, platforms, or protocols [25]. However, because of the generality of the standards, it is difficult to customize them to the particular settings and demands of organizations. The ISO standard demonstrates a close relationship with consistent quality and InfoSec management, whereas the NIST focuses more heavily on operative incident management, which reduces the synergy effects of two aspects: the integration of ISIM into a strategic management system and the systematic knowledge transfer within and between organizations.

In congruence with [16], this study combines the concepts of ISO and NIST into an adapted ISIM. Four phases constitute the framework for the analysis: planning and preparation in phase one, detection and reporting in phase two, analysis and response in

phase three, and learning and improvement in phase four. While phases two and three have a more operative character, phases one and four favor a strategic perspective.

Phase I: Planning and Preparation. During the first phase, organizations establish a solid foundation for systematic ISIM. This basis requires implementing and updating policies regarding InfoSec and ISIM at all organizational levels. The phase specifically considers not only the hardening of the technical part of the information system, which includes devices, applications, and networks, but also the formal rules within and between organizations and the preparation of an incident response team (IRT). Moreover, all employees – whether responsible for ISIM or for other tasks – must be adequately involved and trained to develop proper knowledge of appropriate behavior with regard to InfoSec and ISIM. An organization should consider alternative processes for maintaining critical functionalities, which can interconnect ISIM with continuity management. In addition, this phase implements further tools and rules that are essential for incident detection, analysis, mitigation, and documentation [25]. The phase concludes with proper testing of the functionality of the established means with regard to the technical, formal, and informal parts of the organizational information system.

Phase II: Detection and Reporting. This phase targets the initial phase of an incident, which, apart from the detection of an incident, also includes its initial characterization and reporting. With the aid of the measurements from Phase I, the incident characterization supports the initial estimation of consequences during the first report, which is continuously generated as new results from further activities arise in phase III. The detection of an incident among the large number of warnings that a monitoring system continuously produces requires knowledge and experience within organizations [25]. Achieving an acceptable quality of the information that is manually and automatically collected during this phase facilitates not only further analysis of and response to an incident but also the future development of ISIM. Therefore, comprehensive information should be collected, such as identified vulnerabilities, events, and related decisions. This evidence, apart from enhancing internal ISIM, is also significant for proper reporting of InfoSec-impairing incidents to responsible internal and external stakeholders to inform further decision-making [24]. When the incident type is known, phases II and III are separable in other cases, iterations between these phases can be necessary, particularly when the analyses suggest information that complements the report or detect multiple or subsequent incidents.

Phase III: Analysis and Response. The detected incident undergoes a thorough analysis to determine its character, origin, and consequences. The results of this analysis enable rapid response to the incident and preparation of future routines as well as the improvement of ISIM. A swift reaction can limit the negative consequences and further spread of the incident. In the event that multiple or subsequent incidents arise, the activities of this phase are intertwined and alternate with those of phase II until the incident is finally treated. The policies and processes during phase I constitute the basis of the appropriate proceedings. Similarly, the information that is collected during phase II is input for a proper analysis and response. The analysis assesses the character of the incident and recommends mitigation measures. The response part of this phase then

applies those measures and provides feedback about the success or failure of the treatment. Further improvement of ISIM relies on proper documentation of the incident, the analysis and decision-making process, the measurements, and shortcomings that are identified during the activities in all phases. This input facilitates the development of policies and processes, as the classification of an incident is still subject to development [26]. The aforementioned requirements of the new regulations provide areas for improvement in ISIM, relies on the valuable input of the operative ISIM during the analysis and response phase. The documentation of this phase completes the internal data collection and is a vital precondition for the following activities.

Phase IV: Learning and Improvement. In accordance with the concept of continuous quality management, this phase facilitates developments of InfoSec and ISIM. These developments occur mainly within the organization but can also involve external stakeholders, such as subcontractors, suppliers, or business partners. Involvement depends on the role during the ISIM and the interdependency with organizational processes. While NIST recommends attention to key lessons after each large incident, findings from small incidents should be examined on a regular basis [25]. Organizational learning concerns specific knowledge about incidents, such as the causes of their occurrence or the mitigation activities that were successfully applied or ineffective. The purpose is twofold: to protect the entire information system from similar events and to improve its capabilities for coping with incidents in the future. The results of this phase then inform the activities of the next cycle of ISIM, which begins again with phase I [24]. Phase IV updates the procedures that phase I has defined. These routines address each role in an organization and provide guidance for proper action alongside ISIM, which includes rules about the notification of concerned stakeholders, allocation of appropriate resources, suggested treatment, required documentation, and notification of completion, for example. In addition, the phase extends the compiled documentation on ISIM with information on the maturity of ISIM and organizational knowledge management to enhance both the future performance of ISIM and the inter-organizational collaboration before, during, and after incidents.

2.3 Previous Research

Although a few studies have addressed ISIM in practice, empirical research in this area remains underrepresented, particularly in the context of the GDPR. However, case studies have been performed on ISIM in the energy sector [12, 27] and the oil and gas industries in Norway [28]. Other studies have explored practices in large organizations in, for example, Norway [7] and the finance sector [5]. Further research has investigated the challenges of applying technical solutions for the detection and diagnosis of incidents [29, 30]. Another comprehensive study [31] has applied an integrative perspective of the technical, formal, and informal information system to investigate challenges in IT security management. To date, only one study [16] has investigated the ISIM of IT consulting firms in Sweden with regard to the GDPR and NIS. However, the recent regulations and growing tendency to outsource highlight the subcontractor's role in ISIM as the focus of this study.

3 Methodology

3.1 The Swedish IT Consulting Business Consortium

This study investigates ISIM at three IT consulting firms. These firms are part of a Swedish IT consulting consortium that employs about 2,100 individuals in around 70 companies in Europe. The autonomous subsidiaries, which have 30 employees on average, are based in several countries, such as Germany, Norway, Finland, Denmark, and Sweden. From the Swedish part of the consortium, the parent company and two subsidiaries participated in this study. The parent company (PC) is the head of the IT consulting consortium and has 13 employees, while the first subsidiary (S1) is an IT consulting firm with 135 employees, and the second subsidiary (S2) employs 25 individuals. The selection of these firms ensured appropriate variation, as one of the subsidiaries is close to the average size, but the other is four times larger. Meanwhile, the parent company is half of the average size.

To develop a comprehensive understanding of ISIM in IT consulting firms, this study extends the interview study with a survey. The investigation departs from the literature review, which informed the theoretical framework of both the interviews and the survey [32]. In accordance with [33], this study first selected six individuals who are entrusted with InfoSec and ISIM at the IT consulting firms for the interview study. Table 1 presents the participants, their levels of expertise, and their affiliations. The names of the persons are fictive and gender-neutral to ensure the anonymity of the participants. In the second step, the survey involved 80 employees at S1 with a variety of experience in InfoSec.

Table 1. Selection of interviewees for the study.

Firm	Participant*	Description
Parent company	Mio	Chief InfoSec officer of the IT consulting business consortium for five years; responsible for InfoSec and safety for the entire group
Subsidiary 1	Alex	Consultant manager for 13 years; responsible for safety, security, InfoSec, and management at S1
	Kim	Senior project manager and expert in customer ISIM for three years
	Sam	Specialist for three years in InfoSec and S1's operations
Subsidiary 2	Elia	Consultant manager and successor of Tove; responsible for InfoSec's management for two years
	Tove	Elia's predecessor; responsible for InfoSec and management from 2011 to 2017

* Names are fictive.

3.2 Methods for Data Collection and Analyses

This study employed several methods of data collection and analysis in a mixed methods approach. The initial literature review provided the foundation for the subsequent collection and analysis of empirical material at the IT consulting firms.

The empirical material of this study stems from interviews with the aforementioned individuals, who are responsible for ISIM at their respective companies. In addition, it derives from a survey that was administered to the employees of one of the firms.

In view of the sensitivity of information about InfoSec and ISIM in the work of IT consulting firms, the interviews were conducted individually and in person at each expert's workplace to offer a familiar and comfortable environment for the interviewees. The six interviews lasted nearly one hour on average and were recorded and transcribed with permission to facilitate the subsequent detailed analysis [33]. The semi-structured interviews utilized a questionnaire that departed from the standards and regulations in the ISIM context, which constitutes the theoretical framework of this study. The questionnaire was developed in advance and used open-ended questions to ensure both consistent guidance throughout the interviews and an appropriate openness for encouraging interviewees to describe their experiences from their own point of view and identify challenges that they perceive as particularly important. The classification that emerges from the evidence of this study was also informed by issues that were particularly relevant to ISIM, the GDPR, or the NIS and the position of firms as subcontractors [34].

The survey was created in Google Forms and administered to broaden the knowledge base that resulted from the interview study. The survey addressed employees at IT consulting firms who normally work with tasks other than InfoSec or ISIM duties at their companies. The aim of the survey was to determine the extent of familiarity of the employees with InfoSec and ISIM policies. The survey, which departed from the theoretical framework and results of the interviews, consisted of 11 questions that prompted respondents to grade their knowledge of the variables in Table 2. Four of the survey items were based on a six-point Likert scale ranging from 1 (very limited ability) to 6 (deep knowledge), which forced respondents to opt for one direction by omitting the neutral option [35]. The remaining seven questions were categorical (i.e. yes or no), of which four included an option for ignorance or irrelevance (N/A). The sample of employees was recruited from S1, and the survey was internally distributed by the participant Alex through a link to 80 of the employees. This firm was selected because it has the highest number of employees of the three firms. Forty-seven respondents completed the survey, which translated to a response rate of 58.5%.

During the process of data collection and analysis, the insights from the interviews and survey were mutually supportive and enabled the investigation to achieve proper depth and breadth of understanding of the ISIM of IT consulting firms in light of the new regulations and their particular position as subcontractors. Apart from experiences during the interviews, the analyses were based on recordings, transcriptions, and the answers to the survey questions.

The first part of the analysis concentrated on the evidence of the interview study to clarify the content of the interview material [36] and the challenges with which IT

consulting firms must contend in the context of ISIM. The analysis synthesized the results of the interviews with regard to the four phases of ISIM. Issues that apply to each of these four phases were treated separately. To ensure both proper InfoSec for the participating individuals and companies and adequate validity of the study, the interviewees were invited to review the analysis and the results as well as assist with completing comments. Therefore, the insights emphasize the crucial challenges that the IT consulting firms encountered in their work with ISIM and the new regulations of the GDPR and NIS.

Table 2. Survey items.

Question	Theoretical concept	Variable	Scale
<i>Estimate your level of knowledge about how to ...</i>			
... avoid an ISB*?	ISIM Phase 1	Avoidance	1–6
... detect an ISB?	ISIM Phase 2	PostKNOW	1–6
... decide whether to report an ISB?	ISIM Phase 2	Decide	1–6
How familiar are you with your company's policies for information security?	ISIM Phases 1 & 4	Policy	1–6
Do you experience that GDPR and NIS make it more difficult to decide whether to report an ISB or not?	ISIM Phase 2	Laws	Yes /No / Undecided
Do you know how to report an ISB to your customer?	ISIM Phase 2	HowExt	Yes /No / not relevant
Do you know how to report an ISB in your company?	ISIM Phase 2	HowInt	Yes /No
Would you prefer anonymous reporting of ISBs?	ISIM Phase 2	Anon	Yes /No / Equal
Do you know where you can gain additional information about routines for information security management in your company?	ISIM Phases 1 & 4	Info	Yes /No
Would you hesitate to report an ISB caused by you or your colleague due to negative consequences?	ISIM Phases 2 & 4	NegCon	Yes /No
Do you think you have sufficient knowledge about information security?	ISIM Phases 1–4	KNOW	Yes /No

* (ISB = information security breach)

The survey data were subject to two modes of analysis. First, for the Likert scale items, descriptive data for the total sample were presented in the form of means; for the categorical items, the data were expressed as numbers and percentages of respondents who answered *yes* and *no*. Then, the answers were divided into two parts according to the perceptions of respondents in regard to possessing sufficient knowledge of InfoSec. The *yes* and *no* groups were subsequently compared. Because of the relatively small sample size, the material was subject to a descriptive comparison of means and

groups instead of to inferential statistics. The analysis of the dataset reveals the levels of accurate knowledge among the employees with respect to several aspects of ISIM.

4 Experiences and Challenges in Incident Management

4.1 Perceptions of InfoSec Management Experts

The following sections present the results of the interviews in accordance with the idealized ISIM process that has been presented above. The participants' experiences highlight crucial challenges in the context of ISIM at IT consulting firms due to the new regulations and the firm's particular position. Table 3 summarizes the perceived challenges. The names of the participants are gender-neutral and fictive to ensure their anonymity.

Phase I: Planning and Preparation. The majority of the participants noted an increase in incidents as a major challenge that has accompanied the entry into force of the GDPR. Mio, Sam, and Elia identified the requirement of reporting an incident within 72 h as particularly problematic, which illuminated further obstacles for the organizations. For example, Mio acknowledged that the business consortium had no routine for meeting this requirement at the time of the interview. One reason was that only two employees had comprehensive knowledge of ISIM, which caused delays in their absence. This issue reflects the shortage of experts in the field, which is a major challenge in the context of InfoSec and ISIM.

Alex and Sam identified another challenge in the integration of activities that relate to planning and preparation into day-to-day work. Assigning a person to full-time work in ISIM and InfoSec appeared to be particularly difficult. They acknowledged that those who are responsible for these tasks often have to operate in various roles, which results in procrastination. Both participants also reported challenges of prioritization in InfoSec mostly due to a focus on chargeable hours and costs within IT consulting firms.

Sam emphasized that IT-consulting firms and their customers must be equally aware of the meaning and effects of the regulations. The participant illustrated this challenge with the example of the maintenance of databases containing personal data that are stored at the IT consulting firm to improve the test results of the systems of the customer. Without proper information management, such proceeding may no longer be appropriate according to the GDPR. Sam elaborated that *"many organizations have received a large amount of personal data over time that has been stored elsewhere and thereafter has been forgotten."*

Meanwhile, Kim reported difficulties with understanding the GDPR and observed substantial variation in interpretations and implementations with regard to several factors, especially the assessment and classification of an incident and its severity to decide whether to report it. In this context, Mio and Alex emphasized the significance of establishing service agreements that assign responsibility to the customer.

A lack of proper routines for ISIM appeared to be another challenge in this phase. The adaption of existing processes to the GDPR, the implementation of these adaptations, and the usage of the processes by poorly informed employees are particularly obstructive. To mitigate these issues, Mio acknowledged employee training on incident

reports as a precondition for the implementation of the adapted routines. Kim and Tove have expressed agreement with the benefits of exercising ISIM; however, they also noted difficulty in the preparation and execution of training opportunities due to highly restricted resource allocation.

Such restriction appeared as a reoccurring problem in the ISIM of the IT consulting firms. Although the participants recognized a higher demand for InfoSec from their customers, the firms still struggled to sell this service to their customers or charge a higher amount for work to account for extended security needs. According to the interviewees, the realization that a higher security level may require extra time could arise late and necessitate post-hoc contract extensions. From the perspective of the interviewees, this challenge is critical for IT consulting firms; for example, if the customer encounters an incident within a computer system that the IT consulting firm developed, the event can yield negative consequences for the reputation of the IT consulting firm.

Moreover, Tove indicated that S2 maintains as few devices as possible and noted that the firm lack tools to monitor devices and networks or record incidents. Elia confirmed this remark and specified that the firm is short on qualified personnel in the area of ISIM and consequently a dedicated team for incident response.

Phase II: Detection and Reporting. The uncertainty about both the characteristics of incidents and the details that the employees must report constitutes a major challenge in this phase, according to all participants. As Alex remarked, this uncertainty results in considerable variation in the content of reports. Such individual interpretations have sometimes led to reports on events that can hardly be considered an incident or failure to report a severe incident. Whereas the former creates a large amount of extra work, the latter introduces further problems for analyzing and responding to the incident as well as for the organizational learning and improvement of ISIM. Elia further emphasized the fear of misjudging an incident and its level of seriousness. In the context of GDPR, many participants worried that an incident would later be revealed to be more malicious than initially judged, which might impose costly penalties on the IT consulting firm.

With regard to costs, Sam viewed restricted resources as a barrier to fulfilling the 72-h requirement and explained that an IT consulting firm would balance the costs for extra personnel against the probability that a severe incident will occur. Sam further explained that IT consulting firms may have considerably less time at their disposal, as their position as subcontractors requires that the concerned customer must be involved first. None of the participants mentioned the tightened requirements in the context of the NIS, which requires an initial report to the supervision agency within six hours.

Many of the interviewees perceived major problems with the routines and processes for the detection and reporting phase. Alex expressed general difficulties in developing a process for detection and reporting that could be easily followed by employees while still addressing all of the significant tasks. Otherwise, employees at the subsidiaries would not employ the process. More specifically, Sam and Elia observed a bottleneck in their current process of incident reporting, as only one individual could access reported incidents, which can lead to a serious problem if that person is absent because of, for example, a holiday. Sam added that employees tended to not self-report a

detected incident in the dedicated system and would instead contact Sam to delegate the task of reporting, and Sam would then perform the reporting to ensure a follow-up and later organizational learning. To explain this behavior, Sam referred to a lack of awareness among employees regarding the correct execution of reporting. Kim summarized the behavior of employees at IT consulting firms as follows: *'Often, all employees are so solution-oriented that each solves its own problems but maybe does not report that something has happened.'* According to Kim, such behavior can generate a certain risk if the employee tries to solve the problem in an unsecure manner and is convinced by the result even though the incident actually remains active.

With regard to the GDPR, Mio, Kim, and Elia expected further issues in the detection and reporting phase, as new types of incidents may arise from the extended regulations. Mio imagined two particular obstacles: underreporting because incidents were not identified and overreporting out of fear of making a mistake. Elia reported insufficient clarity of the business consortium's policies, which caused uncertainty among employees with respect to protocol for reporting an incident that concerns customer data. In addition, Tove reported that the PC offers policies that explicitly state that incidents must be reported to the central helpdesk function, which reduces the possibility of handle incidents locally. Tove explained, *"it is some kind of a black hole, because even if we report this way, we do not know if the incident is threatened in an adequate manner."* However, Tove argued that employees should direct questions to their responsible manager and added that employee training has addressed incidents at properties but not InfoSec incidents, which warrant more attention in future employee trainings.

According to Mio, anyone might have to deal with an incident, yet employees may feel embarrassed when they must report an incident. Therefore, the PC seeks to ease this burden for the employees and thereby mitigate the severe consequences that may accompany such behavior. In addition, Sam requested enhanced activities for the detection of incidents that relate to the consortium network. S1 has no possibility of monitoring and controlling the network; therefore, Sam noted that the level of analysis and scan of the network should be heightened, which is ultimately a task of the PC. Mio declared that the PC is generally responsible for ISIM, which applies to all subsidiaries in Sweden. Because of the size of the consortium, its cloud-based data storage is constantly under attack. Therefore, the PC permanently monitors the system of the entire group and filters the incoming warnings, such as those from antivirus software of the clients. Mio acknowledged that it remains uncertain whether the incident will be detected if the antivirus software does not provide an alert. Kim expressed another dimension of the dependency on technology as follows: *"we cannot see if an incident had occurred without an internet connection; we have nothing documented how to act in such situations."*

Phase III: Analysis and Response. The participants revealed immense variation in their perceptions with regard to the analysis and response phase. Mio explained that the PC is responsible for analyzing and mitigating incidents that are manually reported by employees and automatically escalated by the monitoring system. Along with all other issues, the incidents that employees report arise at IT support, which initially assesses the problem. A risk of this proceeding is that it may overlook or delay severe incidents.

Moreover, Mio perceived inadequate experience and knowledge to be other potential threats that can prompt improper decisions, particularly if substitutes must perform the assessment. IT-consulting firms must further contend with their role as subcontractors, as, according to Mio, “*we must always be able to deal with two worlds, our own and our customers’ routines.*”

Although S1 has established routines for this phase, Alex identified two major challenges. First, Alex is solely responsible for the initial assessment of an incident, which includes the decisions of to whom to escalate the incident and which stakeholders to involve. The second challenge is to gauge the extent to which the business should be limited. Alex appreciated that S1 never encountered an incident that affected a customer but imagined that the effects would be even stronger, which Kim also feared. The appropriate balance between continuing the day-to-day business and heightening the level of security is a matter of concern that Sam also noted. In this context, the absence of a common classification scheme was repeatedly deemed problematic. Kim and Sam perceived insufficiency in the policies and documentation with regard to prioritization, escalation, and response, and they demanded clarity about the expected response to several types of incidents. Sam emphasized that such clarified policies must be available, well-known, and practiced by the employees and noted, “*you will never reach the optimal level; it is the striving after balance between risk and measures. Just this point is the state that you never reach but always aim for.*” To reduce the dependency on a single individual who is capable of performing the crucial tasks of analysis and response, S1 was training another person in decision-making regarding technical issues during an incident, according to the participants from S1.

Tove explained that S2, in contrast to the larger S1, delegates the tasks of this phase to the PC and blamed an overall disinterest in these issues and inappropriate focus on costs for this approach. Tove criticized the absence of feedback on incidents that S2 has detected and reported, as S2 consequently does not know when, how, and to what extent the PC has mitigated an incident. In contrast, Mio stated that feedback is regularly returned to the reporting instance. However, Tove imagined that local intermediaries could improve the ISIM process by concentrating attention on important issues and ensuring a rapid response, which may be of particular interest in the context of the GDPR.

Elia recognized further challenges concerning a lack of proper processes and documentation routines for ISIM. Elia suggested an improved structure and thorough documentation of incidents, including “*what we have done...and not only noticing that something has happened*” as well as who has been or must be involved, the applied mitigation activities, and the level of success.

Many of the interviewees indicated that the IT consulting firms tend to apply a stronger focus on security and requirements in relation to customer data and processes, which entails a faster and more comprehensive analysis of and response to incidents that affect customers; meanwhile, they largely disregard their own business.

Phase IV: Learning and Improvement. In general, Mio claimed that the PC has developed an adequate process to both learn from incidents and improve ISIM. Thereby, minor and major incidents are regularly assessed. Yet Mio highlighted the challenge of deciding whether the information should be available for employees with

the same level of details as considered during assessment meetings. According to Mio, the major issue in this regard is to provide an appropriate volume and type of information to ensure that employees continue to take part and do not completely stop reading because the content overwhelms them.

Alex and Kim emphasized the importance of the cross-functional group that S1 has established to discuss incidents during regular meetings. However, they commented that the most thorough discussions focused mostly on major incidents. They both argued that minor incidents or occasional events can provide valuable insight, especially as learning opportunities for avoiding major incidents that can develop from more minor events as well as potential misjudgments in the initial phase. Meanwhile, S2 did not conduct meetings to specifically target incidents or ISIM, according to Tove. Rather, incidents comprised one point of the agenda, which implies insufficient attention to incidents and a lack of organizational learning.

Apart from such meetings, Alex reported the challenge of dedicating time and attention to in-depth learning. Therefore, Alex emphasized an improved flow of information and feedback not only from the meetings to employees but also back. Sam similarly discussed the insufficient feedback from the PC and missed opportunities for learning. Sam also expressed regret that the level of information that is provided about incidents precludes reoccurrences of patterns in attacks on networks. Elia added that inter-organizational communication and the sharing of knowledge about incidents and their mitigation are essential sources of further learning. Tove encouraged a rethinking of systems development: *"When we develop IT systems now so must we have security by default and by design, build in GDPR aspects in the systems and also charging customers for that. So, more focus on all dimensions!"*

Mio perceived another difficulty with regard to knowledge management. Preserving the experiences of an expert in the area of ISIM appeared to be a particular challenge compared to the documentation of external knowledge, such as the detection, analysis, and response to incidents, which Mio considered to be a rather easy task. Mio exemplified the complexities of documenting decision-making during ISIM as follows: *"Why did we make this decision then? Or, why did we this or that? This is much harder to document."*

General Issues. The interviewees emphasized some general issues that can apply to all ISIM phases. All participants acknowledged high awareness among employees and customers as vital for obtaining a proper level of InfoSec and mature ISIM.

The participants reported that employees at IT consulting firms typically possess proper knowledge about InfoSec and technology. However, the majority of the interviewees found it essential to regularly repeat the one-hour InfoSec training, which all new staff members undergo, to maintain awareness and adhere to emerging developments. Tove noted that the content of exercises needs to be updated, and employees should receive reminders on a regular basis; otherwise, InfoSec may be secondary to the core business focus. Sam and Mio imagined that employees' basic knowledge on InfoSec may still be insufficient in regard to contending with advanced and well-performed attacks, which can cause difficulties even for InfoSec experts in detecting an intrusion. According to Mio, the initial assessment and classification of an incident requires appropriate knowledge, especially when it relates to classified customer data,

and escalation needs to target the correct stakeholder. Sam complained of a low maturity level among employees at S1 with regard to the usage of open networks in public spaces. Employees tended to ignore the discussed risks, particularly when using mobile phones or other portable devices. Sam added that employees seemed to understand the value and sensitivity of information when using a computer but not when using a mobile device. Kim confirmed the view that mobile devices are considered more insecure than computers. In addition, the participants at S1 described another challenge in sharing sensitive information, which employees may exchange via e-mail within the organization or with customers. Even if S1 were to handle e-mails securely, the IT consulting firm could not ensure that customers take sufficient care in this respect, so it was impossible for employees to delete sensitive information. The interviewees also related proper customer awareness to the content of the provided information and databases, which attracted further attention in light of the GDPR.

Three interviewees discussed the focus of IT consulting firms on chargeable hours. Alex expressed difficulty with prioritizing InfoSec in daily business operations because InfoSec and ISIM are continuous processes yet are not perceived as central to the firm's business. Sam noted that InfoSec may be a lower priority because the firms concentrate on tasks that are in demand and yield a profit. Sam illustrated the situation as follows: *We are permanently busy and customers are hunting us with a blowtorch...There is an infinite demand of operation and support and this implies that I do not prioritize InfoSec...If you go out to 30 IT firms and ask when they got started with their work on InfoSec, so would all 30 reply that it started after "this" incident.* Tove confirmed this perception and shared that InfoSec is recognized as a support process and was therefore underprioritized by S2 because of cost- and time-related restrictions.

A strong customer orientation accompanies the focus on chargeable services. The interviewees indicated that the preoccupation of IT consulting firms with customer demands has led to a neglect of internal InfoSec demands that, in prolongation, will have repercussions for customers. Alex perceived an eagerness of IT consulting firms to support customers in addressing their problems, which may in turn delay internal efforts toward security, especially when individuals must fulfill several roles. The occurrence of the GDPR recently intensified this challenge, as both IT consulting firms and their customers need to ensure their compliance with the regulation. Elia remarked that this enhanced focus on customer demands also applies to the context of ISIM and the mitigation of incidents that affect customers. Kim expressed that S1 aims for higher accuracy in its assessments of customer systems, which S1 considers more critical than its own systems. Because they expect further business opportunities, such imbalance in assessments is widely accepted by IT consulting firms, noted Kim. Nevertheless, the majority of interviewees indicated that the primary emphasis on fulfilling customer demands has actually prompted improvements to internal InfoSec and ISIM. Customers who demand a high level of InfoSec force IT consulting firms to dedicate efforts to the development of InfoSec management, which regards both customers and internal systems. Sam argued that the management of InfoSec becomes a focus only when it is an inevitability due to, for example, the occurrence of an incident. Kim summarized, *"it seems that we have much more to do in the field of IT security, but it is hard to know exactly what before something has happen."*

Several participants expressed the absence of major incidents as a fortunate circumstance. However, Sam noticed a severe challenge in this lack of experience: employees do not understand the importance of properly reporting incidents for the entire ISIM at S2. Both interviewees from S2 perceived a lack of communication with the PC. For example, Tove emphasized the insufficiency of feedback on how the PC mitigates the reported incidents. In reference to the GDPR, Elia reported ambiguity regarding the extent to which the PC would develop policies for the entire consortium or whether the subsidiaries must create their own.

Table 3. Challenges of ISIM.

ISIM Phase	Challenges perceived by InfoSec managers
I: Planning & Preparation	<ul style="list-style-type: none"> • Avoiding the growing number of incidents related to the GDPR • Shortage of experts and lack of full-time employees for InfoSec • Integrating routines and processes into daily business operations • Understanding the GDPR both internally and externally • Establishing proper customer contracts regarding the GDPR • Creating routines (related to the GDPR) that all employees know and apply • Failure to dedicate training time or trainings to prepare for incidents • Lack of a computer system to record incidents • Absence of an IRT when no employee is qualified to manage incidents • Convincing customers to pay for InfoSec, especially to account for tightened regulations
II: Detection & Reporting	<ul style="list-style-type: none"> • Uncertainty, especially after the GDPR, concerning which events constitute an incident and which information employees must report • Fear of misjudging an incident • Adhering to the requirement of timely reporting (e.g. within 72 h) • No easy and adequate process for incident reporting • Bottleneck in the process of incident reporting • Uncertainty over whom employees should contact in the event of an incident that affects a customer • Embarrassment of reporting incidents • Insufficient system scanning from the central level
III: Analysis & Response	<ul style="list-style-type: none"> • Escalation of incidents • Lack of knowledge and training, especially among substitutes • Gauging the extent to which daily business operations must be tightened in case of an incident and particularly if it affects a customer • Limited policies and routines to guide employees in acting and prioritizing various types of incident • Ensuring that policies about routines and processes are available, known, and practiced • Inadequate documentation of incidents and mitigation activities • No local analysis or response because of costs, which must be changed

(continued)

Table 3. (continued)

ISIM Phase	Challenges perceived by InfoSec managers
	<ul style="list-style-type: none"> • Lower security consideration and prioritization of internal data and incidents compared to external issues, i.e. data and incidents that relate to a customer
IV: Learning & Improvement	<ul style="list-style-type: none"> • Balancing the content and scope of employee information for enhancing awareness of, commitment to, and compliance with policies • Misjudging minor incidents or extraordinary events that have the potential to become an incident • Lack of meetings dedicated solely to incidents • Allotting sufficient time to thoroughly review incidents • Information sharing among all personnel • Lack of feedback from the central level on incidents that relate to networks • Insufficient external communication and knowledge sharing • Organizational knowledge and experience management
General Issues	<ul style="list-style-type: none"> • Obtaining a high awareness of InfoSec among customers and employees • Focus on chargeable hours, which hampers the implementation of continuous InfoSec work • Excessively strong customer focus, which neglects internal demands • Lack of (experience with) major incidents • Insufficient communication with the parent company

4.2 Knowledge of InfoSec Among Consultants

Tables 4, 5, and 6 contain the results of the survey, which are based on the variables from Table 2 (Y = Yes, N = No, U = undecided, not relevant, equal) in Sect. 3.2. As noted, 47 employees of S1 completed the survey. Of those respondents, only 12 (25.5%) perceived their knowledge of InfoSec to be sufficient. As evident in Table 4, the means of this group (“KnowYES”) were higher than those of the other group (“KnowNO”) for all Likert scale items.

Table 4. Survey results: means and standard deviations.

Question	Total (n = 47)	KnowYES (n = 12)	KnowNO (n = 35)
Avoidance	4.49 ± 0.9	4.83 ± 0.58	4.37 ± 0.97
PostKNOW	3.77 ± 1.13	4.42 ± 0.52	3.54 ± 1.2
Decide	3.89 ± 1.1	4.33 ± 0.89	3.74 ± 1.12
Policy	3.68 ± 0.96	4 ± 1.2	3.57 ± 0.85

Table 5 reveals that many respondents were undecided on effects of the GDPR and NIS, which might be explained by the relative newness of the laws. Most respondents knew how to report an incident to a customer. A majority were indifferent toward the anonymous reporting of incidents, although 21.3% would prefer anonymous reporting. The “KnowYES” group yielded a slightly higher number of “YES” responses compared to the “KnowNO” group (see Table 5).

Table 6 indicates that a majority of respondents (89.4%) knew where to acquire information about routines for InfoSec management in the IT consulting firm. Moreover, despite potential negative consequences for themselves or their colleagues, the same percentage would not hesitate to report an incident. A majority (93.6%) was also aware of how to internally report an incident. Nevertheless, as the results in Table 5 demonstrate, the respondents indicated lower confidence (70.2%) in regard to incidents that affect customers. The “KnowYES” group displayed slightly higher values compared to the “KnowNO” group with respect to these variables as well.

Table 5. Survey results from questions with three choices.

Question	KnowYES (n = 12)			KnowNO (n = 35)			Total (n = 47)		
	Y	N	U	Y	N	U	Y	N	U
Laws	2	7	3	3	13	19	5	20	22
	16.7%	58.3%	25%	8.6%	37.1%	54.3%	10.6%	42.6%	46.8%
HowExt	9	1	2	24	9	2	33	10	4
	75%	8.3%	16.7%	68.6%	25.7%	5.7%	70.2%	21.3%	8.5%
Anon	3	2	7	7	4	24	10	6	31
	25%	16.7%	58.3%	20%	11.4%	11.4%	21.3%	12.8%	66%

Table 6. Survey results from questions with three choices.

Question	KnowYES (n = 12)		KnowNO (n = 35)		Total (n = 47)	
	Y	N	Y	N	Y	N
Info	11 (91.7%)	1 (8.3%)	31 (88.6%)	4 (11.4%)	42 (89.4%)	5 (10.6%)
NegCon	1 (8.3%)	11 (91.7%)	3 (8.6%)	31 (88.6%)	4 (8.5%)	42 (89.4%)
HowInt	12 (100%)	0 (0%)	32 (91.4%)	3 (8.6%)	44 (93.6%)	3 (6.4%)

5 Characterization of InfoSec Incidents

In the interviews, the decision of whether an incident warrants reporting arose as a reoccurring challenge. The results of the survey further illustrate that IT consulting firms lack knowledge of the character of incidents. The interviewees sought to enhance employee awareness through training scenarios regarding, for example, how to react when a mobile phone is lost or a power failure occurs at the office; still, the timely recognition of incidents remained a challenge. The interviews revealed the following several dimensions that can characterize an incident.

- Organizational level: whose area of responsibility is affected?
- Security level: which level of InfoSec applies, and which requirements exist?
- Knowledge level: which previous knowledge exists about the incident?
- InfoSec attribute: which InfoSec attribute is affected?
- Concerned asset: which asset is affected?
- Time frame: when did the incident start, and how long has it been underway?
- Propagation: how quickly does the incident propagate?
- Impact: what is the scope of effects?
- Mitigation: To what extent must measures must be taken?
- Severity: how serious is the incident?

Comprehensive documentation throughout the ISIM process must collect additional data about mitigation measurements, involved expertise, and the eventual level of success. The evaluation of a finally treated incident should then take account of the consequences, including costs and savings, possible alternative proceedings, and the decision-making process that was applied. Implementing a method for a structured decision analysis could enhance decision-making about future mitigation measures should a similar incident occur.

An incident classification can facilitate a comparison of emerging incidents and their treatments with previously handled instances. Moreover, it can provide a benchmarking tool for IT consulting firms in their ISIM evaluations, which consider not only costs for preventing and mitigating incidents but also possible alternative endings. Thus, such assessments indicate the benefits of vigorously acting InfoSec management and ISIM. The proposed classification scheme in Table 7 assigns several attributes to each dimension of an incident. These attributes constitute a scale from zero to five for each dimension, whereby zero signifies a very mild type of an incident and five represents a worst-case scenario. An incident at zero may concern a public document that fell on the ground on its way to the bin; such case can be easily mitigated

and does not require reporting. If one or more dimensions appear to be unknown, then the incident ascends in the ranking. Accordingly, if no dimension is known, then the detected incident would score a five, which would require full efforts – at least initially – for mitigating the incident. An incident's ranking can be adjusted as new information becomes available.

Table 7. Classification scheme of InfoSec incidents.

Dimension	Attributes
Organisational level	0-none, 1-local, 2-subsiary, 3-business group, 4-customer, 5- N/A
Security level	0-public, 1-internal, 2-restricted, 3-confidential, 4-secret, 5-N/A
Knowledge level	0-very high, 1-high, 2-medium, 3-low, 4-very low, 5-N/A
InfoSec attribute	0-none, 1-availability, 2-integrity, 3-confidentiality, 4-privacy, 5-N/A
Concerned asset	0-property, 1-device, 2-network, 3-human, 4-data, 5-N/A
Time frame	0-seconds, 1-minutes, 2-hours, 3-days, 4-months, 5-N/A
Propagation	0-very slow, 1-slow, 2-medium, 3-quick, 4-very quick, 5-N/A
Impact	0-very limited, 1-limited, 2-serious, 3-major, 4-massive, 5-N/A
Mitigation	0-documented, 1-basic, 2-multiple, 3-advanced, 4-extensive, 5-N/A
Severity	0-marginal, 1-minor, 2-critical, 3-major, 4-catastrophic 5-N/A

In addition to incident classification, IT consulting firms can establish particular thresholds regarding reporting requirements or who is permitted and responsible for mitigating incidents of various levels. Such thresholds could respond to particular dimensions or a cumulative index that specifies the threat level of the incident. For this purpose, the attributes can be cumulated in several ways, including the use of statistical measures, such as the mode, mean, or median, and weighted measures.

The classification of InfoSec incidents can support further opportunities for IT consulting firms. For example, it could allow the compiled documentation of incidents to be searchable for different incident types, which would in turn enable internal and external auditors to assess and evaluate emerging incidents, dedicated mitigation efforts, established policies and routines, and the entire ISIM. Such concentrated assessment could inform improvements to InfoSec in general and ISIM in particular as well as local, internal, and inter-organizational learning (Fig. 1).

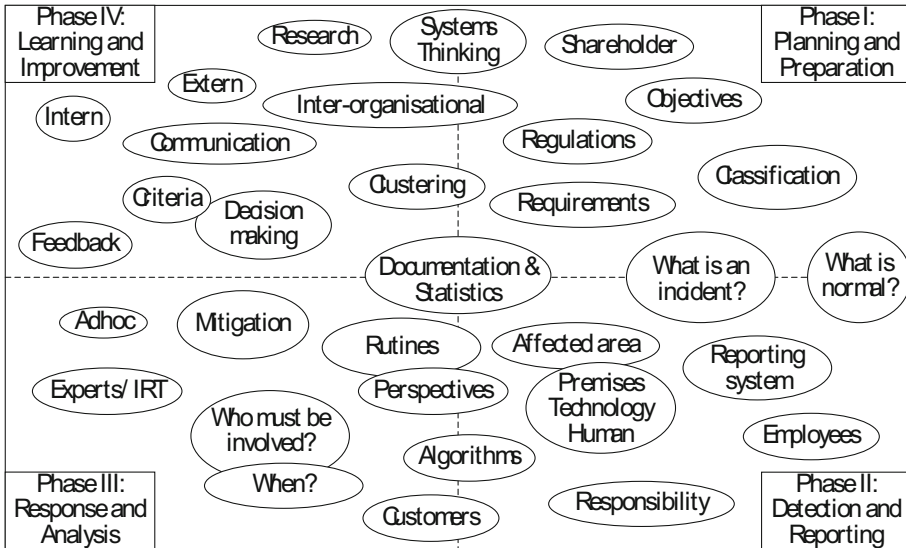


Fig. 1. Activities, means, and stakeholders that can be informed by a structured classification and documentation of InfoSec incidents

Prolonged and widespread use of a similar classification scheme could additionally facilitate the development of an incident database in which incidents and mitigation measures are searchable and comparable. Such database could also contribute local, regional, national, and international statistics about the branch, severity, and types of incidents, for example, which can equip scholars and practitioners to conduct further research and development.

6 Implications

The results of this study demonstrate that ISIM poses a variety of challenges for IT consulting firms. Such challenges have a broad range of possible consequences for the business operations of both IT consulting firms and their customers. This study of Swedish IT consulting firms has identified particular issues that reoccurred in several contexts and thus warrant certain attention:

1. Fixation on costs
2. Trust in technical measurements
3. Lack of documentation
4. Low understanding of and adaption to legal regulations
5. Poor inter-organizational communication and collaboration
6. Insufficient knowledge of the character and proper treatment of incidents.

First, the fixation on costs led to constant oversight of the benefits of proper InfoSec for companies in terms of reducing the negative effects of an incident. Therefore, the

findings support the results of [31], which has indicated that costs can easily outrank InfoSec and structured ISIM as a priority. As [27] has also illustrated, such diminished importance of InfoSec further lowered the attention to preparing and executing employee training for improving ISIM. This study noted the consequences of such preoccupation with costs in the smaller subsidiary, S2, which manifested in the insufficiency of documentation, processes, personnel, and technical support for ISIM. Another issue that accompanied the cost focus is that individuals at IT consulting firms valued ISIM of customer systems more highly than that of their own systems. Such imbalance may yield additional severe consequences, such as damage to reputation or customer relations, if an incident propagates across systems. Therefore, the new regulations require more attention to a comprehensive risk analysis for InfoSec.

Second, this study has declined the argument of [30, 31] that the character and number of warnings of monitoring systems cause difficulties. Instead, it is necessary to question the minimization of the number of warnings by filter mechanisms. For example, in the present study, the PC monitored the entire system of the consortium and purchased the filtering of warnings. In combination with a minimized number of system scans, these measures produced a manageable number of warnings. However, this trust in technical measures can be dangerous, as it may allow incidents to proceed undetected for an unwanted period and thereby deliver massive consequences. This study has further indicated that subsidiaries lack knowledge of specific results of the monitoring. Therefore, employee awareness can benefit from improved modes of communication and knowledge transfer with regard to the limitations of automatized monitoring. According to the interviewees, the rarity of experts in InfoSec also represents a challenge, as their well-documented knowledge can become an increasing challenge in a situation that requires specific competence and experience [29].

Third, as noted above, a lack of documentation hampered any structured ISIM within organizations or in inter-organizational cooperation. Previous research, international standards, and best practices have continuously advocated for proper documentation of incidents and the ISIM process. However, this study reveals that the maturity of the documentation remains significantly low, which constitutes a massive challenge in the ISIM of IT consulting firms. Such inadequacy of documentation accompanies the insufficiency of knowledge about the following aspects: the importance of documentation; policies, processes, and regulations; the designation of responsibility within the organization and in cooperation with external stakeholders; how to report and which aspects to include [7]; how to analyze and respond to incidents, especially major ones [28]; and the means of documentation, communication, and feedback.

This study has demonstrated uncertainty among InfoSec experts and employees that may relate to the lack of knowledge and documentation in IT consulting firms. Therefore, the proposed characterization scheme in this study can support improvements. This incident classification can be a catalyst for ISIM in its entirety by facilitating more structured documentation, which involves not only a characterization of the incident but also details about its mitigation and the underlying decision-making process. Comprehensive documentation must include the best treatment and success factors while also elaborating on poor decisions and failures to enhance learning within and between organizations. The results particularly encourage employee trainings that

focus on secure practices with respect to mobile devices and their use within public networks. In addition, the model for characterizing incidents can impart structure to meetings for discussing certain events and minor incidents, which reflects another means of enhancing awareness, compliance, and competence.

Fourth, the individuals at IT consulting firms mentioned a major challenge that relates to the tightened regulations of the NIS and GDPR, which amplified uncertainty among both the employees and the individuals who are responsible for ISIM. Despite such ambiguity in interpreting the legal requirements, the policies, routines, and agreements with customers and subcontractors must adapt to current and further developments of the regulations. This study recognizes that IT consulting firms extensively focus on the GDPR as well as the avoidance of costly penalties for inadequate compliance. Moreover, the results of this study reveal an exclusive concentration on the GDPR and complete neglect of the importance of the NIS for the ISIM of IT consulting firms. Apart from the scarcity of experienced personnel in the field, the fixation on costs can be another impactful factor for such orientation, as the GDPR threatens severe penalties, whereas the NIS does not.

Fifth, this study evidences that decision making about serious measures to mitigating an incident, such as the shutdown of a customer system, was perceived as an uncomfortable assignment that requires stable inter-organizational relations. Even though the results emphasize the significance of InfoSec, daily business operations seek to continue service provision with as few disturbances as possible. The inherent ambiguity of this discrepancy complicates decision-making about adequate measures and, when necessary, communication with the concerned customer and supervision agency. Although this study could not investigate such trustful relations in practice, one of the participants acknowledged the potential for inter-organizational sharing of experiences and knowledge. In such context, the proposed characterization scheme could facilitate a structured exchange and offer a benchmark regarding incidents and mitigation measures. Meanwhile, the assignment of corresponding attributes during incident classification can limit access to more detailed documentation. Such enhanced exchange of knowledge through statistics and documentation could improve inter-organizational relations and ISIM at participating organizations.

Finally, uncertainties about the character of an incident and its correct management emerged as central challenges in the ISIM of IT consulting firms. Participants were particularly concerned with the detection of an incident, which includes the realization of a difference from the normal state. Their uncertainty also encompassed knowledge of when, what, how, and to whom an incident should be reported as well as the necessary mitigation measures. Such confusion and lack of knowledge implies that policies and employee training are absent, insufficient, or improperly understood among employees [7, 12]. The findings of this study indicate that employees tended to underpredict seemingly minor incidents [5, 27]. Therefore, such types of incident mitigation could illustrate how to prevent a minor incident from developing into a serious one. The lack of experience with serious incidents at the participating IT consulting firms may have expounded their ignorance of such learning opportunities. In addition, the cost focus may be another reason for this underestimation of minor incidents. The results demonstrate the difficulty of retaining expert knowledge in the organization. In addition to simultaneously involving novices and experts in the mitigation process to learn

practices from each other [31], the proposed incident characterization scheme combined with detailed descriptions of concrete activities, including their level of success, could facilitate the establishment of a structured documentation base that allows for knowledge transfer and benchmarking.

7 Concluding Remarks

This study has contributed valuable knowledge to the field of InfoSec and on ISIM at IT consulting firms in particular. First, to address the lack of empirical studies in this context, the results provide insight into experiences and challenges in ISIM at a Swedish consortium of IT consulting firms. The inquiry has particularly examined their specific position as subcontractors. The findings of the interviews with InfoSec experts in the firms and a survey with employees at one of the selected subsidiaries have accentuated practical challenges of ISIM. The main concerns were an obsession with costs, a lack of adequate policies, guidelines, processes, and documentation, and insufficient knowledge of the character of an incident and its proper treatment. The lack of experience with managing major or catastrophic incidents in combination with the recent GDPR and NIS regulations pose a massive challenge for IT consulting firms. The matter of proper interpretation and fulfillment of requirements, such as timely reporting to a supervision agency, the customers of the IT consulting firms, or both, appears to be as critically concerning as the appropriate distribution and balance of responsibilities between the firms and their customers.

This paper has proposed a new classification scheme with 10 criteria, which were substantiated by the findings of the empirical investigation. Applying these criteria to an event provides a solid basis on which decision-makers can assess the incident management. This model for classifying an incident constitutes a tool for comparing emerging incidents and their treatments. Thus, the model can also offer a benchmarking tool for other organisations than IT consulting firms to evaluate their ISIM.

Further developments in theory and practice can support the implementation and improvement of the classification scheme in a variety of contexts and organizations and by involving a larger number of participants. Nevertheless, the enhanced understanding of ISIM challenges for IT consulting firms in regard to their specific position as subcontractors as well as the model to classify InfoSec incidents both provide valuable insights for organizations that seek to improve their ISIM in developing internal and inter-organizational processes.

References

1. Blix, F.: 1177-leak in Sweden: 2.7 million recorded healthcare phone calls leaked online (complete write-up). <https://www.linkedin.com/pulse/1177-leak-sweden-27-million-recorded-healthcare-phone-fredrik-blix>
2. Sones, M.: Sweden accidentally leaks nearly all citizens' personal details. <http://www.israelnationalnews.com/News/News.aspx/233057>

3. The Local Sweden: Swedish authority handed over ‘keys to the Kingdom’ in IT security slip-up. <https://www.thelocal.se/20170717/swedish-authority-handed-over-keys-to-the-kingdom-in-it-security-slip-up>
4. Olsson, J.: Svenska Kraftnät medger säkerhetsbrister. <https://www.svt.se/nyheter/inrikes/svenska-kraftnat-medger-sakerhetsbrister>
5. Ahmad, A., Hadgkiss, J., Ruighaver, A.B.: Incident response teams – challenges in supporting the organisational security function. *Comput. Secur.* **31**, 643–652 (2012)
6. Ab Rahman, N.H., Choo, K.-K.R.: A survey of information security incident handling in the cloud. *Comput. Secur.* **49**, 45–69 (2015)
7. Hove, C., Tärnes, M., Line, M.B., Bernsmed, K.: Information security incident management. Identified practice in large organizations. In: Freiling, F. (ed.) 8th International Conference on IT Security Incident Management and IT Forensics, pp. 27–46. IEEE, Piscataway (2014)
8. Tøndel, I.A., Line, M.B., Jaatun, M.G.: Information security incident management Current practice as reported in the literature. *Comput. Secur.* **45**, 42–57 (2014)
9. Cusick, J.J., Ma, G.: Creating an ITIL inspired incident management approach. roots, response, and results. In: Gaspary, L.P. (ed.) 2010 IEEE/IFIP Network Operations and Management Symposium workshops, pp. 142–148. IEEE, Piscataway (2010)
10. Bailey, J., Kandogan, E., Haber, E., Maglio, P.P.: Activity-based management of IT service delivery. In: Kandogan, E. (ed.) Symposium on Computer Human Interaction for the Management of Information Technology. ACM, New York (2007)
11. European Union (EU): Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016)
12. Line, M.B.: A case study. Preparing for the smart grids - identifying current practice for information security incident management in the power industry. In: Morgenstern, H. (ed.) 7th International Conference on IT Security Incident Management and IT Forensics, pp. 26–32. IEEE, Piscataway (2013)
13. O’Brien, R.: Privacy and security. *Bus. Inf. Rev.* **33**, 81–84 (2016)
14. Swedish Civil Contingencies Agency (MSB): Årsrapport it-incidentrapportering 2018. En sammanställning och analys av de statliga myndigheternas it-incidentrapportering (2019)
15. Swedish Civil Contingencies Agency (MSB): Årsrapport it-incidentrapportering 2016 (2017)
16. Nyman, M., Große, C.: Are you ready when it counts? IT Consulting firm’s information security incident management. In: Proceedings of the 5th International Conference on Information Systems Security and Privacy, pp. 26–37. SCITEPRESS - Science and Technology Publications (2019)
17. International Organization for Standardization (ISO): ISO/IEC 27000:2018
18. Große, C.: Towards an Integrated Framework for Quality and Information Security Management in Small Companies. Luleå (2016)
19. European Union Agency For Network and Information Security (ENISA): Guidance and gaps analysis for European standardisation. Privacy standards in the information security context (2018)
20. Tankard, C.: What the GDPR means for businesses. *Netw. Secur.* **2016**, 5–8 (2016)
21. European Union (EU): Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (2016)
22. Swedish Civil Contingencies Agency (MSB): Vägledning om rapportering av incidenter för leverantörer av digitala tjänster enligt NISregleringen. MSB 2018-13472 (2018)

23. Swedish Civil Contingencies Agency (MSB): Nationellt system för it-incidentrapportering (2012)
24. International Organization for Standardization (ISO): ISO/IEC 27035:2016. Information technology – Security techniques – Information security incident management (2016)
25. Cichonski, P., Millar, T., Grance, T., Scarfone, K.: NIST 800-61, Revision 2: Computer Security Incident Handling Guide. National Institute of Standards and Technology, Gaithersburg (2012)
26. European Union Agency For Network and Information Security (ENISA): Reference Incident Classification Taxonomy. Task Force Status and Way Forward (2018)
27. Bartnes, M., Moe, N.B., Heegaard, P.E.: The future of information security incident management training. A case study of electrical power companies. *Comput. Secur.* **61**, 32–45 (2016)
28. Jaatun, M.G., et al.: A study of information security practice in a critical infrastructure application. In: Rong, C., Jaatun, M.G., Ma, J., Sandnes, F.E., Yang, L.T. (eds.) *Autonomic and Trusted Computing*, 5060, pp. 527–539. Springer, Berlin (2008). https://doi.org/10.1007/978-3-540-69295-9_42
29. Werlinger, R., Muldner, K., Hawkey, K., Beznosov, K.: Preparation, detection, and analysis. The diagnostic work of IT security incident response. *Info. Manage. Comp. Secur.* **18**, 26–42 (2010)
30. Werlinger, R., Hawkey, K., Muldner, K., Jaferian, P., Beznosov, K.: The challenges of using an intrusion detection system. In: Cranor, L.F. (ed.) *Proceedings of the 4th Symposium on Usable Privacy and Security*, p. 107. ACM, New York (2008)
31. Werlinger, R., Hawkey, K., Beznosov, K.: An integrated view of human, organizational, and technological challenges of IT security management. *Info. Manage. Comp. Secur.* **17**, 4–19 (2009)
32. Bryman, A., Bell, E.: *Business Research Methods*. University Press, Oxford (2015)
33. Denscombe, M.: *The Good Research Guide. For Small-Scale Social Research Projects*. McGraw-Hill Education, Maidenhead (2014)
34. Johannesson, P., Perjons, E.: *An Introduction to Design Science*. Springer, Cham (2014). <https://doi.org/10.1007/978-3-319-10632-8>
35. Croasmun, J.T., Ostrom, L.: Using likert-type scales in the social sciences. *J. Adult Educ.* **40**, 19–22 (2011)
36. Schutt, R.K.: *Investigating the Social World. The Process and Practice of Research*. Sage, Thousand Oaks (2015)