Conflict Resolution in an ISO/IEC 27001 Standard Implementation: A Contradiction Management Perspective

Wael Soliman
University of Agder
wael.soliman@uia.no

Anniina Ojalainen
Government ICT Centre Valtori
anniina.ojalainen@valtori.fi

Abstract

The ISO/IEC 27001 standard provides organizations with guidelines to help them evaluate, document, and improve their information security processes. In practice, however, the generality of the standard can create a conflict between its requirements and the adopters' expectations. To better understand how an organization manages such conflicts, we conduct a case study in a Finnish corporation during the standard's implementation in one of its units. Two critical conflicts emerged: Conflict I reflects a tension between the standard requirement for disciplinary measures vis-à-vis the organization's punishment-averse culture. Conflict II reflects a tension between the organization's aspiration for concrete code reviewing instructions vis-à-vis the lack thereof in the standard. Our findings reveal that whereas the conflict resolution process was similar in managing both conflicts, their content was radically different. Specifically, whereas conflict I's resolution was paradoxical, conflict II's resolution was dialectical. We discuss the theoretical and practical implications of our findings.

Keywords: ISO/IEC 27001, conflict resolution, paradox, dialectics, contextualism.

1. Introduction

With increasing dependency on information and information systems (IS), protecting organization's cyber environment and information assets has become a much-needed organizational capability. One common approach for attaining and maintaining the needed capabilities is to pursue an information security (InfoSec) management standard certification, which is considered one of the most widely used security management methods (Siponen, 2005). Standards vary considerably in terms of popularity and focus, and some of the most well-known standards include the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27001, the National Institute for Standards and Technology Special Publication (NIST SP) 800-series, the Payment Card Industry Data Security Standard (PCI-DSS), and more recently, the General Data Protection Regulation (GDPR), to name a few.

Unfortunately, however, the often lengthy and iterative process of planning, implementing and adopting an InfoSec standard can make it an extremely confusing experience filled with conflicts and tensions, and in the end, many organizations fail to achieve their objectives with the standard adoption (Culot et al., 2019; Hsu, 2009; Karyda et al., 2005). One of the most recognized limitations of security standards, such as ISO/IEC 27001 (2013), is that they generally focus on ensuring that certain InfoSec controls and processes are in place; yet they do not provide clear guidance regarding how these controls and processes are translated into 'situated practice' (Niemimaa & Niemimaa, 2017). This challenge has long been recognized in the InfoSec literature where the standards' focus often lies in the existence of *process* but not and its *content*, which may promote a false sense of security (Siponen, 2006).

Considering this growing challenge, recent research calls have encouraged researchers to pay more attention to the importance of context and content and focus on in-depth experiences and lessons learned from the various InfoSec standard implementation projects (Culot et al., 2019; Niemimaa & Niemimaa, 2019). In response, in this article we adopt a contextualist approach (Pettigrew, 1985, 1990) and report our findings from a case study where we explore how an organization managed to resolve two challenging conflicts that arose during an ISO/IEC 27001 standard implementation. *Conflict I* demonstrates a tension between the standard requirement for disciplinary measures *vis-à-vis* the organization's egalitarian and punishment-averse culture. *Conflict II* demonstrates a tension between the employees' aspiration for clear software code reviewing guidelines *vis-à-vis* the ambiguity within

URI: https://hdl.handle.net/10125/103223
978-0-9981331-6-4

the standard. Our findings reveal that whereas the conflict resolution process was similar in managing both conflicts; their content were radically different. That is, whereas the resolution to conflict I has been *paradoxical* in nature, the resolution to conflict II has been predominantly *dialectical* (Hargrave & Van de Ven, 2017; Smith & Lewis, 2011).

2. Theoretical background

Security standards come in various forms; the two most common genres are the technically-oriented and the managerially-oriented standards (Hsu, 2009; Karyda et al., 2005). On one hand, a technology-oriented standard addresses the technical specification of a given technology/product, such as, the ETSI EN 303 645 (V2.1.1) standard, which provides baseline requirements for cybersecurity in Internet of Things (IoT) devices. On the other hand, management-oriented standards, such as the ISO/IEC 27001 standard, are mainly concerned with guiding organizations (and their members) to formulate and operate their InfoSec efforts. This article focuses on the management-oriented standards. At their core, these InfoSec standards (and the guidelines therein) are meant to be "international, authoritative and generic" (Siponen, 2005, p. 305), and in that sense, they are written in an abstract language so that they can be generalized to any type of organization in any context. No doubt, these InfoSec standards play a crucial role in helping many organizations protect the confidentiality, integrity, and availability of their information assets. However, due to their generalizability objective, they also tend to focus on process (i.e., what needs to be done) at the expense of content (i.e., how it can be done; see Siponen, 2006); thus, setting the stage for tensions to materialize between what an organization expects from the standard and what the standard offers.

Recognizing this challenge, we adopt a contextual perspective which recognizes that (organizational) change involves a "continuous interplay between ideas about the *context* of change, the *process* of change, and the *content* of change" (Pettigrew, 1985, p. 62). These three core facets of change form the foundation of our theoretical framework. The notion of context is central since it sensitizes us to the importance of potential tensions arising from conflicts between the outer and inner contexts. In line with this understanding, Soliman and Rinta-Kahila (2020) describe context as the organizational environment and the background story in which the change processes take place. In our analysis, context reflects the unique background information where change is taking place.

The second defining element in our framework is the process. Process is defined as "a continuous, interdependent, sequence of actions and events which is being used to explain the origins, continuance, and outcome of some phenomena" (Pettigrew, 1985, p. 64), which, in our case, is reflected by the ISO/IEC 27001 implementation journey. Considering that our approach explicitly embraces explanation via contradiction (*vis-à-vis* consensus-seeking, see Robey & Boudreau, 1999), we focus on the process of conflict resolution (i.e., contradiction management). The contradiction management literature emphasizes the occurrence of the three core stages: (1) *tension materializing*, (2) *sensemaking*, and (3) *resolution* (Hargrave & Van de Ven, 2017; Karjalainen et al., 2019; Niemimaa & Niemimaa, 2019). Furthermore, the literature points to at least four broad categories of tensions, namely, learning tensions, belonging tensions, organizing tensions, and performing tensions (Smith & Lewis, 2011), each of which addresses a set of contradictions or dilemmas that permeate organizational life. In our case, the contradiction management lens will help us understand how the case firm managed to cope with conflicts that have arisen from incongruencies between the ISO/IEC 27001 requirements and the firm's culture and unique demands for software development.

The final defining element in our framework is content, which refers to the rich insights we learn from the phenomenon under study. Content is often defined slightly differently depending on the study context and the key aspects believed to be relevant to that study. For instance, in Napier et al.'s (2011) contextualist analysis, content referred to "areas being transformed", which in their case, focused mainly adaptability and alignment (p. 677). In our study, content is seen as the narrative that describes particularities of conflict-resolution to better understand how the case firm has managed to navigate the standard implementation successfully. despite the challenging conflicts that arose. Two key areas are of interest: (a) the conflict between the disciplinary requirements of ISO/IEC 27001 and the organizational sanction-aversion culture, and (b) the conflict between the need for code reviewing process and the lack of clear guidance in the standard.

3. Empirical study

In this case study, our primary aim is to make sense of how the ISO/IEC 27001 implementation process unfolded over time. Consistent with the interpretive research tradition in IS (Walsham, 1995, 2006), our emphasis is on understanding how conflicts arose and how they were resolved from the study

participants' point of view (Hargrave & Van de Ven, 2017). Considering the unique focus of our research, we were fortunate to connect with an organization that had just acquired a smaller firm and was in the process of preparing it for the ISO/IEC 27001 implementation and auditing processes. More importantly, the organization welcomed us to conduct the research after discussing our general objectives. Due to the sensitive nature of their operations, the organization requested to remain anonymous, and therefore we will refer to the parent organization as *Corporate X*, and its newly acquired software development unit as *SD Unit*.

Both Corporate X and SD Unit operate in ICT in Finland. Corporate X provides ICT services, mainly in the private Business-to-Business (B2B) domain, whereas the SD Unit specializes in software development. Importantly, at the time when we started the research collaboration, Corporate X was already ISO/IEC 27001 certified, while the SD Unit was not.

In this dynamic context, we decided to focus our attention on the ISO/IEC 27001 implementation process within the newly acquired SD Unit as experienced by its own members. Before the acquisition, the SD Unit had a small team of software developers who created their own processes and policies. After the corporate acquisition, the newly acquired SD Unit had to align their procedures to that of Corporate X's. As we will reveal later, the employees in the SD Unit had mixed feelings about the acquisition. On the one hand, as a part of a bigger company, they would be better positioned to win more competitive tendering, and they would also gain more resources and expertise from the parent organization. On the other hand, they must comply with to the Corporate X's operations and policies, which translates to less independence on their decisions and way of working.

3.1. Data collection

Two rounds of interviews were conducted between February 2020 and September 2020 with employees who were intimately versed in the ISO/IEC 27001 implementation process at the research site. Altogether, 22 semi-structured interviews (Myers & Newman, 2007) were conducted with 11 employees at different organizational levels. In the SD Unit, 7 study participants held positions as software developer/coder, while 3 participants held managerial/supervisory positions. Each interviewee was interviewed twice (i.e., once at every interview round). The study participants had tenures in the organization between 18 months to 16 years, and everyone was familiar with the organization's policies and processes. In addition to the interviews with the SD Unit employees, we also interviewed Corporate X's Chief Information Security Officer (CISO) to give us an overview of the organization and the SD Unit's acquisition process. Two lengthy interviews were held with the CISO, and additionally, several phone calls were made to clarify any uncertain matters.

The interviewing process may be divided into two distinct rounds; each focusing on a different aspect of the events that took place before and after the ISO/IEC 27001 standard audit. In the first interview round, ten interviews were conducted at the SD Unit to gain an overall understanding of the corporate acquisition and the goal of the ISO/IEC 27001 auditing process. Some of the central questions in the first interview round included (among others): *How familiar are you with current security policy? What motivates you to adhere to the organization's security policies? How do you think the ISO/IEC 27001 standard certification would affect your daily work?*

The interviewees were given the freedom to describe their experiences in their own words and were encouraged to reflect on any interesting issues they might have. Although our initial interest was on better understanding the challenges that might arise with the disciplinary measures' implementation, it was during the first interview round that we recognized that the SD Unit's bigger concern was their quest for concrete guidance regarding the code reviewing process. The majority of the interviewees described how they struggled to fulfil the standard requirements which did not fit their small development team straightforwardly. In addition, they described how they were especially disappointed in the lack of secure development practices related to code review process.

Having identified these two specific challenges/conflicts (namely, disciplinary measures and code reviewing), in the second interview round, our objective was twofold. First, to probe whether employees' attitudes towards the security policy and the ISO/IEC 27001 standard implementation have changed over time. Second, to gain in-depth understanding of the strategies the organization adopted to resolve these conflicts that emerged. To this end, we interviewed the same employees to understand how the ISO/IEC 27001 implementation was fulfilled, how the employees resolved the challenges that arose during the implementation process, and how the overall experience was after the audit process.

Upon interviewees' consent, all interviews were audio-recorded, transcribed verbatim, and then transcripts were translated from Finnish to English by one of the authors, who is a native Finnish speaker, to make sure that the resultant translations captured the essence of what was communicated during the interview sessions.

3.2. Data analysis

Our data analysis relied on two main strategies, namely, temporal bracketing (Langley, 1999) and thematic analysis (Braun & Clarke, 2006). On the one hand, temporal bracketing enabled us to pay attention to the dynamically developmental nature of conflict resolutions, so we placed the core activities of the standard implementation in a logically temporal order along three stages: *(a) pre-implementation planning and formulation, (b) implementation and guidelines translation, and (c) post-implementation outcomes* (Karyda et al., 2005). Thematic analysis, on the other hand, helped us to identify the salient themes pertaining to explaining conflict materialization and resolution.

The main objective of conducting thematic content analysis was to link the themes and interviews together under a category system (Attride-Stirling, 2001). All interview transcripts underwent thematic analysis where color coding was used to organize similar phrases and paragraphs under common themes and patterns (Saaranen-Kauppinen & Puusniekka, 2009). For example, the reported attitudes toward disciplinary measures were color coded in *yellow*, the emerged conflicts were coded in *red*, and the identified resolutions were color coded in *green*. This coding process served as a foundation to identify and label the most salient themes affecting the standard implementation.

Furthermore, the three concepts of context, content and process were kept in mind throughout the whole data analysis. First, the notion of context helped us focus on the environment where the change was taking place. For instance, attention to context made us take note of the importance of the organizational history and relationship between Corporate X and the acquisition deal over the SD Unit. Second, the notion of process sensitized us to the importance of studying the employees' evolving experience with the implementation process at various points in time. Third, content directed our attention to (a) focus on specific conflicts within the implementation process (which we label *Conflict I* and *Conflict II*), and (b) to pay careful attention to the fine details of how these conflicts were resolved. Importantly, consistent with the hermeneutic orientation of interpretive research, reaching our findings was a highly iterative process that involved going back and forth between the empirical data and the literature, until we reached an illuminating and plausible explanation (Mees-Buss et al., 2022, p. 421).

Finally, we find it important to clarify that in our analysis of conflicts and resolutions, we made a conscious effort to avoid making value judgements about decisions surrounding the standard implementation process. For instance, questions regarding whether the decisions taken by the organizational members were right or wrong, solid or baseless, are beyond the scope of our analysis.

4. Findings

We begin by reporting a brief background information to situate the implementation process in its context. As noted earlier, the SD Unit was acquired by Corporate X to complement its increasing software development needs. After the acquisition, all the employees of the newly acquired SD Unit got to keep their old positions. Naturally, the interviewees (belonging to the SD Unit) expressed mixed feelings related to the corporate acquisition, but we could see that the general atmosphere was mainly positive. However, the same cannot be claimed about ISO/IEC 27001 implementation. The dominant posture toward the ISO/IEC 27001 standard was not optimistic. The biggest source of tension was the general attitude that the ISO/IEC 27001 standard was not compatible with a software development environment. For instance, the employees that were handling the implementation and auditing process expressed their frustration with the fact that they had to speculate the ISO/IEC 27001 standard's requirements on a daily basis. They felt that the requirements did not straightforwardly transfer to their software development environment, and this caused conflicts between their daily operations and the standard documentation.

Our analysis points to two of the biggest tensions the employees working with ISO/IEC 27001 implementation faced, namely: *(a) the disciplinary measures* and *(b) the code reviewing process*. On the one hand, the ISO/IEC 27001 standard universally requires documenting and communicating disciplinary measures (Annex 7.2.3). Most interviewees argued that such disciplinary measures did not fit well in their organization, nor in the Finnish work culture in general. On the other hand, issues with the code reviewing process were brought up by more than half of the interviewees as a challenge deserving careful attention. In practice, the code reviewing processes needed to be organized to increase InfoSec and overall security of the software, but many employees believed that the ISO/IEC 27001 standard did not clearly articulate the requirements or processes related to software development in action (Annex 14.2.1). While it is not necessarily the standard's responsibility to provide such detailed guidance for code reviewing; it was nonetheless remarkable to observe that this issue created yet another tension.

Next, we report our findings and elaborate how these two tensions emerged and were resolved from the interviewees' point of view.

4.1. Conflict I: Disciplinary measures

Disciplinary measures are a common component of any InfoSec policy denoting that section of the policy that describes various types and levels of sanctions to be applied on those who violate the policy. Disciplinary measures range from verbal or written warnings, salary deductions, all the way to terminating employment and even pressing criminal charges. While sanctions have different purposes (Gibbs, 1975), the deterring effect of sanction is what concerns most InfoSec researchers (Trang & Brendel, 2019), based on the assumption that fear of punishment will deter employees from violating the stated rules (Balozian & Leidner, 2017; Siponen et al., 2021).

Stage 1: Pre-implementation (planning)

Prior to the acquisition deal, the SD Unit had developed its own InfoSec policy, which made no mentioning of disciplinary measures. Ignoring the disciplinary measures entirely is a problem from the ISO/IEC 270001 standard's standpoint, which in practice, could mean failing the certification process. In essence, the standard's Annex A.7.2.3 emphasizes that that there needs to be a documented disciplinary process for InfoSec breaches/violations which must be communicated to the employees. Therefore, the discussion of disciplinary measures was brought in the implementation process.

Discussing this dilemma with the interviewees was carefully planned as we sought to understand the interviewees' general attitude towards sanctions and disciplinary measures, as well as to explore the scenarios in which they believed such measures may be acceptable or even necessary. During the interviews, it became evident that the interviewees thought that disciplinary measures would not motivate employees, especially in a Finnish organization context operating in a creative field. To them, applying disciplinary measures would disrupt the sense of safety which enabled the employees to be creative and take initiatives, and jeopardizing this dynamic could be disruptive. Employee 4 described their view on disciplinary measures as follows:

> *"Disciplinary measures would affect us in a way where we would not dare to do our work in the same way anymore or take responsibility of things. It would make my view of the employer very negative and if we would be threatened with disciplinary measures, I might even consider cancelling my contract of employment in that situation."* -Interviewee 4 [Coder]

The managers we interviewed seem to share the employees' point of views on disciplinary measures. In fact, all three managers considered that disciplinary measures would hamper the workplace's morale. One manager clearly expressed this view:

> *"Disciplinary measures would extremely negatively affect people. We are in the creative field and have a smart and educated team. If leading would happen through communicating punishments, the negativity of it would spread to the whole working environment."* -Interviewee 10 [Manager]

Even further, another manager argued that, in their experience there were often good reasons behind non-compliant behavior, and that a good manager should be able to notice the warning signs forcing employees to violate the policy. They explain:

> *"It is not natural for me to rely on disciplinary actions. I always try to think of something else first. On the other hand, as a supervisor I think there is always something else behind non-compliant behavior that I should have been able to detect. A good supervisor can notice that this person is not going in the right direction. I do not think that punishment is a good way to handle these situations. Not the best motivational tool. It even weakens the work atmosphere."* -Interviewee 6 [Manager]

Stage 2: Implementation (documenting)

The SD Unit was handling the disciplinary measure documentation as required by the ISO/IEC 27001 standard. One of our key questions was to figure out whether the interviewees were aware of the existence of a disciplinary documentation process taking place during stage 2 (implementation and documentation), and more importantly, to what extent they were made aware of any new sanctions or disciplinary measures being introduced for violating the InfoSec policy. Surprisingly, it became clear that the interviewees were neither aware of a disciplinary process documentation taking place, nor of any new sanctions were being introduced. Interviewee 5 provides an illustrating example:

> *"I have never heard of disciplinary actions. There has not been communication about them that I would have internalized. I could imagine that a supervisor should communicate these measures to us. I have no clue if we would have any sanctions of information security policy violations."* -Interviewee 5 [Coder]

Stage 3: Post-implementation (certification)

The lack of awareness among the SD Unit employees does not mean that Corporate X has disregarded the disciplinary measures requirement from their documentation process. Doing so would have meant failing the ISO/IEC 27001 auditing and certification processes, which they passed effortlessly. To us, this was a rather thought-provoking dilemma: on the one hand, the SD Unit employees seemed to

lack any knowledge of disciplinary measures, and on the other hand, the ISO/IEC 27001 auditing process was successful, and the certification was granted. How did Corporate X resolve this dilemma?

The interviews revealed a remarkable resolution: Corporate X arranged for the disciplinary measures documentation to be handled without inconveniencing the SD Unit employees with the process formalities. Talking with Corporate X's CISO, it became apparent that the disciplinary measures were handled at the corporate level only, and that the documentation was discreetly made available in the organization's internal website. In that sense, Corporate X's resolution struck a compromise between the ISO/IEC 27001 requirements for explicit documentation and communication of disciplinary measures on the one hand, and on the other hand, keeping the employees' sense of safety unjeopardized. To satisfy the standard requirements, Corporate X had handled the documentation of the processes, but the disciplinary measures and processes were never communicated to its intended audience.

We challenged the interviewees to think of situations where they considered disciplinary measures acceptable. Interestingly, the examples they gave described serious criminal situations in which the employee would be breaking the Finnish Legal Code. In less serious cases, the dominant opinion was that disciplinary measures were unnecessary and even demotivating. As such, the interviewees seemed to believe that the application of disciplinary measures was only justified if the employee's InfoSec policy violation broke a clearly stipulated law.

Eventually, the organization resorted to what is best described as a co-persistent resolution (i.e., a paradox): To meet the ISO/IEC 27001 requirements, disciplinary measures were developed, documented, and published on the organization's internal website. At the same time, to keep the employees' morale uncompromised, the disciplinary measures were neither enforced nor communicated in practice.

4.2. Conflict II: Code reviewing

Code reviewing is a common software quality assurance practice, whereby the software code being developed undergoes various testing and auditing activities from internal or external members of the development team. The literature points to two broad approaches to the code review processes: *ad-hoc/irregular* and *change-based/regular* review processes (Baum et al., 2016). The first approach points to industry practices where the software code reviewing processes are initiated and performed on irregular basis and are often driven by individual needs. The second approach points to practices that are more systematic and rule-based. For example, in such processes, the code reviewing is codified in the development process of the development team, and every time a unit of work (e.g., part of a code) is seen as ready for review, all changes from the previous unit are assessed. If the review is seen as necessary, the work unit waits for the reviewers to evaluate the code (Baum et al., 2016). Regardless of which review approach an organization adopts, the quality assurance of software development is crucial when delivering secure software and ICT services.

Stage 1: Pre-implementation (planning)

Focusing on the code reviewing process was not initially a planned interview theme, however, it emerged during as one of the main concerns troubling the interviewees during the first interview round. For instance, over half of the interviewees brought up their worries related to their organization's code reviewing process (or the lack thereof). The discussions revealed that, prior to the acquisition, the SD Unit once had in place a rather complicated internal code reviewing process, which was later abandoned due to its burdensome and arbitrary nature. As such, the employees were rather dissatisfied with the *status quo* regarding how such a core process as code reviewing was (mis)handled. One programmer described their experience as follows:

> *"As we are doing software, the code reviewing process could be better. It could be handled in a way where you are forced to go through the reviewing process. Now, the organization just trusts that someone will go through the code. The code reviewing usually is eventually done but there is still an opportunity that you forget it, or it just gets ignored."* -Interviewee 3 [Coder]

Discussing the prospects of implementing the ISO/IEC 27001 standardization, the interviewees expressed some concerns, mainly in terms of the burdensome that comes with systematicity. For instance, Interviewee 7 expressed some worries regarding the additional time that would be required to review colleagues' code and that this would *"make everything slower"*. Despite this, the interviews indicated that the overall attitude towards the upcoming ISO/IEC 27001 implementation was generally positive, especially based on the promise that the standard would provide them with clear guidance on making their code reviewing processes more systematic. Interviewee 7, who had some worries about the burdensome of systematicity, noted:

> *"We had code reviewing processes before, but it was so burdensome, it became voluntary. … There is no systematicity. Because of ISO/IEC 27001 implementation, we will go towards the systematic approach again … I hope the new process will cost itself back so there will be less issues coming from the customers' end."* -Interviewee 7 [Coder]

Stage 2: Implementation (documenting)

The ISO/IEC 27001 standard dedicates Annex A.14.2. to describing its security requirements in development and support processes. Its general objective (Annex A.14.2.) is to ensure that security is designed and implemented within the development lifecycle of information systems. Strong signs of tensions started to materialize when the employees' aspirations for clear guidance were met with what they perceived as abstract and ambiguous guidelines. Based on the interviews, it became evident that once the actual implementation began, the employees (who were initially excited about the ISO/IEC 27001 implementation) started to realize the tension between expectations *vis-à-vis* reality, especially when it came to translating the standard's requirements into actions. Employee 7 explains their newfound frustration:

> *"This whole ISO/IEC 27001 implementation is insanely heavy. It feels like you are more than half the time guessing what these requirements mean in practice. ISO/IEC 27001 specifications are so circularly written that there can be no concreteness about what needs to be done correctly. Those different interpretations go all over the place, and we go through the same things repeatedly. This is an energy consuming task. I wish we had someone who could explain the standard from a software development perspective."*

Another participant – Interviewee 2 [Coder] – revealed that they frequently found themselves at a loss when they needed to grasp what the ISO/IEC 27001 standard required of them. In the same vein, reflecting on the implementation process, a manager in the SD Unit expressed their dismay with the ambiguity in the language used in the standard, and especially the fact that it required substantial interpretation from the implementers' part, noting the following:

> *"[The] ISO/IEC 27001 standard did not state how the code reviewing process should be handled, but then, it did not tell us anything practical, anyway. The standard does not seem to comment on how things should be done. You just have to hope your solution fits the requirements in the end."* -Interviewee 10 [Manager]

Stage 3: Post-implementation (certification)

Interviews targeting the post-implementation stage revealed that the code reviewing processes had passed the auditing, but to our surprise, we learned that the once-frustrated employees now seemed to be more satisfied with the new process and they considered it a major improvement over the old ways of working. We found this development very interesting, so we delved further into how they managed to resolve this dilemma; namely, the conflict between their aspiration for a detailed code reviewing guidance and the vagueness of the ISO/IEC 27001 guidelines.

It became apparent to us that the employees' approach to resolving the dilemma is best described as *"educated guessing"*. In fact, the employees were not sure if their guesses were right until they passed the standard auditing process. For example, six of the ten interviewees expressed their puzzlement regarding the lack of concrete measures that address code reviewing processes. These employees pointed out that the ISO/IEC 27001 standard would only hint that the code reviewing may rely on some well-known mechanism or vulnerability lists, without detailing what these mechanisms or lists could be. To resolve this dilemma, the implementation team had to speculate (i.e., make an "educated guess") what this could mean to the best of their knowledge. This quest led them to adopt the OWASP Top 10 Security Risks (www.owasp.org) as a basis to tailor their own code reviewing process. One interviewee described their experience as follows:

> *"ISO/IEC 27001 does not give an opinion on code reviewing process, but it hints that your processes should rely on some well-known mechanisms. So, then we concluded that it is worth relying on known vulnerability lists. We did not interpret the standard, but rather just speculated it. Apparently, our speculation turned out to be right."* -Interviewee 7 [Coder]

Employees who were involved in this guesswork or speculation expressed their experience as very stressful and tiring. Nonetheless, after the successful completion of the documentation and certification, not only were they relieved, but also, they had concrete knowledge of the code reviewing best practices. In effect, the interviewees were now familiar with the details of their new code reviewing process and were also able to clearly articulate what needed to be done, when, and by whom. An interviewee describes the new code review process as follows:

> *"Before [the] ISO/IEC 27001 implementation, we had to review [the] code that was made in different projects, and it was hard to find time for it. Now we have designated code reviewing pairs who take care of the code reviewing when it is their turn. … The process is not too heavy, and it has already become a routine for me. We get an automated message from the version control program when we need to review someone's code. If we still forget to do it, our team leader will remind us of it. … I think we have learned from our previous mistakes."* -Interviewee 1 [Coder]

Furthermore, the employees seemed to appreciate the fact that the ISO/IEC 27001 standard demanded that organizations provide evidence of the security measures they have implemented. Before the implementation, the review process was done on an ad-hoc basis, and the SD Unit had no such trail – even among the same team members – that any code reviewing was indeed carried out. Now the situation has changed as an interviewee describes it:

"*Before, we did not have any proof that the code reviewing was carried out. Now we can prove that the code reviewing is done because you have to check off that you have done it and then there is a record left of it for everyone to see."* -Interviewee 3 [Coder]

Overall, despite the ISO/IEC 27001 standard's lack of clear guidance, all the interviewees described the new code reviewing process as a major improvement. In fact, even though the interviewees saw the new process to be more time-consuming, they were now confident that it increased their security posture, and in the long term, this time spent would pay off, for example, there would be less future security vulnerabilities requiring patching.

5. Discussion and concluding remarks

5.1. Theoretical elaboration

In this case study, we set out to explore how an organization managed to resolve tensions that arose during its security standard implementation, taking into consideration the uniqueness of its context: an egalitarian Finnish organization operating in the creative domain of developing ICT solutions. Our analysis points our attention to the salience of two critical tensions in the *performing* and *organizing* domains (Smith & Lewis, 2011). On one hand, tensions in the disciplinary measures requirement strongly resonate with performing tensions. They typically "stem from the plurality of stakeholders and result in competing strategies and goals" (Gibbs, 2009, p. 384), which in our case points our attention to the organization's effort to find a middle ground between the standard's requirement for control and punishment, and the internal expectations for freedom and creativity. On the other hand, tensions in the code reviewing process provide a clear example of organizing tensions. They typically occur when "complex systems create competing designs and processes to achieve a desired outcome" (Gibbs, 2009, pp. 383-384), which in our case points our attention the pursuit of concrete measures for a secure code reviewing process.

In terms of process, our findings are consistent with the contradiction management literature which emphasize the occurrence of the three core stages: *tension materializing* → *sensemaking* → *resolution* (Hargrave & Van de Ven, 2017; Karjalainen et al., 2019; Niemimaa & Niemimaa, 2019). For instance, we could clearly observe in our case that the resolutions to both conflicts engendered a form of *abductive innovation* (Niemimaa & Niemimaa, 2019) concluding the search for a middle ground between *deductive adoption* (i.e., the ISO/IEC 27001 official security requirements) and *inductive adjustment* (i.e., the real-life business demands). However, despite the general consistency between the tension-resolution process and our findings, the most revealing insights are in the content of this process, most notably, in terms of the nature of resolution itself, which we discuss next.

When focusing on the nature (i.e., content) of tension resolution itself, the literature points to various archetypes of responses or resolutions, such as, selection, separation, integration/synergy transcendence/synthesis (Gibbs, 2009; Jarvenpaa & Wernick, 2011; Karjalainen et al., 2019; Smith & Lewis, 2011; Tracy, 2004). Interestingly, our case analysis reveals that the organization's handling of conflicts arising from the ISO/IEC 27001 implementation demonstrates two clearly distinct strategies to resolving conflicts I and II. That is, whereas conflict I's resolution may be described as *paradoxical*, the resolution to conflict II is best described as *dialectical*.

A *paradoxical resolution* in an organizational setting occurs when its members find a way to accept the coexistence of contradictory elements and "manage them through a combination of differentiation and synergy, rather than trying to resolve the tension between them" (Hargrave & Van de Ven, 2017, 320). Corporate X's approach to resolving the tension between the ISO/IEC 27001 requirement for disciplinary measures and the dominant punishment-averse culture in the SD Unit is an excellent example of a paradoxical resolution. In effect, the organization decided to both *adopt* and *reject* the disciplinary measures requirement. On one hand, documenting and publishing the disciplinary measures on the organization's intranet is a clear sign that these measures have been *explicitly adopted*. On the other hand, this adoption is only superficial since these measures were neither enforced, nor communicated to the employees, which is a clear sign that, in practice, the management decided to *implicitly reject* the disciplinary measures. However, implicitly rejecting organizational disciplinary measures does not mean that the organization wishes to operate in an unruly environment. For instance, they clearly respect and uphold the law and would gladly comply with disciplinary measures when an employee's behavior violates the legal code. Instead, they do not see value in introducing the fear of punishment to govern their creative environment which embraces experimenting, and trial and error. This resultant resolution is merely a way to live with the contradictions, and lacked any sign of transcendental/transformative qualities, which is more evident in the organization's response to conflict II.

A *dialectical resolution*, in contrast, is transcendental in that its occurrence requires the

merging of a thesis and its antithesis. The collision between the two opposite poles creates a new synthesis (i.e., a transformation in the form of a dissolution), which, given the time, it stabilizes and becomes the new thesis (Hargrave & Van de Ven, 2017; Van de Ven & Poole, 1995). In our case, the organization's response to resolving the tension between the employees' expectations for concrete guidance for code reviewing on one hand, and the lack thereof in the ISO/IEC 27001 standard, on the other, is a clear example of synthetic innovation (Niemimaa & Niemimaa, 2019). Interestingly, one of the biggest tensions that arose in the SD Unit was not caused by the InfoSec standard's stringent or strict requirements, as is often the case. Rather, the tension arose because the ISO/IEC 27001 was rather vague/lax at a time when the employees were aspiring for clarity and concreteness. Unlike the resolution to conflict I, where the measures were superficially adopted, the employees genuinely believed that they needed to devise a (re)solution to improve the security posture of their code reviewing process. Employees at the SD Unit had to speculate (i.e., make educated guesses) about what the ISO/IEC 27001 requirements were and what they actually needed in the workplace, and it was in this alternation between deductive adoption (i.e., the thesis) and inductive adjustment (i.e., the antithesis) that a synthetic innovation emerged (i.e., synthesis). In this sense, we agree with Niemimaa and Niemimaa's (2019) notion that a dialectical (re)solution is about "finding innovative ways that could be taken neither directly from the best practices, nor from local practices" (p. 576).

5.2. Practical implications

The insights presented thus far point to very important practical implications. Clearly, the ISO/IEC 27001 standard implementation can be a tedious task for the implementing organization and its members. Many of the participants brought up the challenge of interpreting the standard's imprecise requirements, which they viewed as a stressful and frustrating ordeal. In the end, they managed to acquire the certification, but in retrospect, many of the interviewees mentioned how they would have benefitted from more support from the parent company or from an external consultancy to guide them throughout the process. At the same time, the interviewees were also aware that a coach from Corporate X or a third-party consultant could have introduced additional challenges since they might not be familiar with the unique requirements of software development and its creative nature. Interestingly, their skepticism resonates with Culot et al.'s (2019) finding which suggest that an external consultant may hinder organizational learning and lead to unsuccessful standard implementation.

Our work addresses unique conflicts that the employees had to resolve to translate the standard into daily operations. Conflicts can be managed in multiple ways, but the paradoxical and dialectical approaches discussed earlier suggest that reaching a resolution and restoring equilibrium may take more than a single path. One path can be through fusing the polarities causing the tension so that they create a new and unified way of working. Another path may be through keeping the old and new ways separate where they can pick what they need to pass the certification without putting effort in introducing new ways of working. Both management styles can lead to a successful implementation and certification, but the focus should be on how the different approaches might affect the organizational culture and its context of operations.

Finally, our work points to an important practical question worthy of future investigation. How detailed should information security management standards be? Certainly, we do not expect of the ISO/IEC 27001 standard, or any information security management standard for that matter, to provide detailed instructions for how the standard should be implemented in different contexts, since it is incredibly challenging to create instructions that fit all organizations of different sizes, cultures, and areas of businesses. But is there room for improvement? One area worth considering is to steer the standards into the direction that provides real-life examples of how the requirements could (rather than should) be actualized. For example, the National Security Authority of Finland has created an InfoSec audit tool (Katakri 2020) which has proved beneficial to both security practitioners and implementing agencies. While the tool focuses on general baseline security requirements (e.g., security management, physical security, and information assurance), the tool also manages to give implementation examples of every requirement listed. With the help of such supporting tools, organizations can decide themselves if they will follow the standard's examples or if they rather determine them their own way.

6. References

27001, I. (2013). *ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements*.

Attride-Stirling, J. (2001). Thematic networks: An analytic tool for qualitative research. *Qualitative Research*, *1*(3), 385–405.

Balozian, P., & Leidner, D. (2017). Review of IS security policy compliance: Toward the building blocks of an IS security theory. *Data Base for Advances in*

Information Systems, *48*(3), 11–43.

Baum, T., Liskin, O., Niklas, K., & Schneider, K. (2016). A Faceted Classification Scheme for Change-Based Industrial Code Review Processes. *IEEE International Conference on Software Quality, Reliability and Security (QRS)*, 74–85. https://doi.org/10.1109/QRS.2016.19

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing industry 4.0 cybersecurity challenges. *IEEE Engineering Management Review*, *47*(3), 79–86.

Gibbs, J. (2009). Dialectics in a global software team: Negotiating tensions across time, space, and culture. *Human Relations*, *62*(6), 905–935.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. Elsevier.

Hargrave, T. J., & Van de Ven, A. H. (2017). Integrating dialectical and paradox perspectives on managing contradictions in organizations. *Organization Studies*, *38*(3–4), 319–339. https://doi.org/10.1177/0170840616640843

Hsu, C. W. (2009). Frame misalignment: Interpreting the implementation of information systems security certification in an organization. *European Journal of Information Systems*, *18*(2), 140–150.

Jarvenpaa, S. L., & Wernick, A. (2011). Paradoxical tensions in open innovation networks. *European Journal of Innovation Management*, *14*(4), 521–548.

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Information Systems Research*, *30*(2), 687–704.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: A contextual perspective. *Computers and Security*, *24*(3), 246–260.

Langley, A. (1999). Strategies for theorizing from process data. *Academy of Management Review*, *24*(4), 691–710.

Mees-Buss, J., Welch, C., & Piekkari, R. (2022). From templates to heuristics: How and why to move beyond the Gioia methodology. *Organizational Research Methods*, *25*(2), 405–429. https://doi.org/10.1177/1094428120967716

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26.

Napier, N. P., Mathiassen, L., & Robey, D. (2011). Building contextual ambidexterity in a software company to improve firm-level coordination. *European Journal of Information Systems*, *20*(6), 674–690. https://doi.org/10.1057/ejis.2011.32

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

Niemimaa, M., & Niemimaa, E. (2019). Abductive innovations in information security policy development: an ethnographic study. *European Journal of Information Systems*, *28*(5), 566–589.

Pettigrew, A. M. (1985). Contextualist research and the study of organizational change processes. In E. Mumford, R. Hirschheim, G. Fitzgerald, & T. Wood-Harper (Eds.), *Research Methods in Information Systems* (pp. 53–78).

Pettigrew, A. M. (1990). Longitudinal field research on change: Theory and practice. *Organization Science*, *1*(3), 267–292.

Robey, D., & Boudreau, M. C. (1999). Accounting for the contradictory organizational consequences of information technology: Theoretical directions and methodological implications. *Information Systems Research*, *10*(2), 167–185.

Saaranen-Kauppinen, A., & Puusniekka, A. (2009). *"Menetelmäopetuksen tietovaranto KvaliMOTV." Kvalitatiivisten menetelmien verkko-oppikirja. Yhteiskuntatieteellisen tietoarkiston julkaisuja*.

Siponen, M. T. (2005). An analysis of the traditional IS security approaches: Implications for research and practice. *European Journal of Information Systems*, *14*(3), 303–315.

Siponen, M. T. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, *49*(8), 97–100.

Siponen, M. T., Soliman, W., & Vance, A. (2021). Common misunderstandings of deterrence theory in information systems research and future research directions. *The DATA BASE for Advances in Information Systems*.

Smith, W. K., & Lewis, M. W. (2011). Toward a theory of paradox: A dynamic equilibrium model of organzining. *Academy of Management Review*, *36*(2), 381–403. https://doi.org/10.5465/AMR.2011.59330958

Soliman, W., & Rinta-Kahila, T. (2020). Toward a refined conceptualization of IS discontinuance: Reflection on the past and a way forward. *Information & Management*, *57*(2), 103167. https://doi.org/https://doi.org/10.1016/j.im.2019.05.002

Tracy, S. J. (2004). Dialectic, contradiction, or double bind? Analyzing and theorizing employee reactions to organizational tension. *Journal of Applied Communication Research*, *32*(2), 119–146. https://doi.org/10.1080/0090988042000210025

Trang, S., & Brendel, B. (2019). A meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers*, 1265–1284.

Van de Ven, A. H., & Poole, M. S. (1995). Explaining development and change in organizations. *Academy of Management Review*, *20*(3), 510–540.

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems*, *4*, 74–81.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320–330.