Dec 11th, 12:00 AM

Designing Extended Zero Trust Maturity Model – From Technical to Socio-Technical

Simen Tokerud
Department of Information Systems, tokersim@gmail.com

Jarand Nikolai Jansen
Department of Information Systems, jarandjansen182@gmail.com

Marko Niemimaa
University of Agder, markoin@uia.no

Jonna Järveläinen
University of Turku, Turku School of Economics, jonna.jarvelainen@utu.fi

Recommended Citation

Tokerud, Simen; Jansen, Jarand Nikolai; Niemimaa, Marko; and Järveläinen, Jonna, "Designing Extended Zero Trust Maturity Model – From Technical to Socio-Technical" (2023). *Rising like a Phoenix: Emerging from the Pandemic and Reshaping Human Endeavors with Digital Technologies ICIS 2023*. 5.
https://aisel.aisnet.org/icis2023/cyber_security/cyber_security/5

Designing Extended Zero Trust Maturity Model – From Technical to Socio-Technical

Completed Research Paper

Simen Tokerud
TietoEvry
Kjøita 6, 4630 Kristiansand
simen.tokerud@tietoevry.com

Jarand Jansen
Orkla
Drammensveien 149, 0277 Oslo
jarand.jansen@orkla.no

Marko Niemimaa
University of Agder
Postboks 422, 4604 Kristiansand
marko.niemimaa@uia.no

Jonna Järveläinen
University of Turku
Rehtorinpellonkatu 3, 20540 Turku
jonna.jarvelainen@utu.fi

Abstract

Recent successful cybersecurity attacks have exploited trust to compromise organizational information systems. Scholars and practitioners agree that the issue originates from the organizational perimeter security approach, within which perimeter trust is assumed. To improve the situation, building security principles on the idea that trust is not inherent but earned has been proposed, coined as Zero Trust. However, the current discussions spearheaded by technology-minded practitioners have focused mostly on trust at the network security and architecture levels, largely omitting the organizational aspects of security. To address this gap, we build on socio-technical approach and maturity models to develop a novel artifact with security experts, addressing the need for organizational Zero Trust through the Extended Zero Trust Maturity Model. Our research contributes to discussions on holistic information security management by extending the principles of Zero Trust from technical into socio-technical approach and responds to calls to reconsider foundational assumptions of IS security.

Keywords: Zero Trust, Cybersecurity, Maturity Model, Design Science

Introduction

> *"That I don't trust anyone does not mean that I suspect anyone either"* – An anonymous Information Security Manager

Organizational responses advocated by practitioners and scholars to occasions when employees have been exploited to carry out cyberattacks have been to increase security awareness, training, and education. This has been enforced through stricter information security policy compliance using coercive, deterrent, and persuasive approaches (Cram et al. 2019). On the other hand, more technology-oriented scholars and practitioners have started questioning the foundational architectural ideas around which information security is built (Buck et al. 2021). According to this perspective, the problem is not merely how technologies are developed, built, and deployed but rather the foundational principles upon which information security has been built.

This traditional way of building information security, including network defense and security architecture, has been to build defense largely on the organizational outer perimeter and assume that everything inside the perimeter is trusted (Whitman 2003). To use the analogy of an old castle, the defense is built on the high walls, fences, and moats around the castle, but those inside the walls are treated mostly as trusted citizens. This analogy has largely dominated the way information security has been built in organizations for decades (Dlamini et al. 2009).

New information security principles have been advocated by the more technology-oriented practitioners referred to commonly as Zero Trust (Buck et al. 2021). Zero Trust is not a technological solution per se nor any specific approach but centered around the core principle that trust should not be assumed but earned. While this idea may sound like a small shift, it has profound implications for how information security is organized. The perimeters are no longer treated as the last (and only) line of defense; there should be no difference between that which is "external" and "internal" either physically or logically.

However, given its origins, it is hardly a surprise that much of the discussions on the application of Zero Trust have centered on technical aspects of information security despite that several studies and surveys point to the criticality of the employees in the protection of organizational information (Buck et al. 2021). Consequently, there is a need to study how the Zero Trust principles could be extended from technical to socio-technical.

One way to operationalize the Zero Trust principles into more concrete organizational guidance has been to develop maturity models. Several proprietary and vendor-dependent maturity models exist that focus on the technical aspects of information security, e.g., on the technological implementation of access control and network security. Following Thuan et al. (2019) guidelines for design science research questions, we pose the question of "How can we incorporate a socio-technical approach/principles to design an artifact of the Zero Trust maturity model?". We employ a design science research approach to design jointly with information security experts an Extended Zero Trust Maturity Model (EZTMM) and evaluate its organizational applicability and usefulness through a naturalistic case study.

Knowledge Base

While security technologies continue to play a crucial role for organizations in their efforts to protect the information, several researchers have pointed to the significance of approaching security holistically (Soomro et al. 2016). This means addressing not just the technologies but also the organizational aspects, e.g., policies, processes, procedures, and human behavior (Choobineh et al. 2007). Broader information systems (IS) literature has long recognized the interplay and reciprocity between the social and the technical aspects of organizing known as the socio-technical approach (Mumford 2006). Key to the socio-technical approach is the recognition that any changes to technical aspects of organizing always necessitate changes in the social aspects. Also, in the context of information security, Coles-Kemp (2009) argues these two aspects are so tightly connected that the technical is inseparable from the social and that they jointly produce contingent security outcomes. Despite the insights from the socio-technical approach, technologists tend to treat technologies as isolated and independent of the social implications and impact they may yield (technology neutrality). Given its origins in the technology-minded practitioners, it is thus not a surprise that also Zero Trust has largely adopted the technology view and treated it isolated from the organizations and the context of its implementation (Buck et al. 2021). We adopt a socio-technical view of information security in order to extend Zero Trust from a technology to an organizational approach.

Scholars have proposed various frameworks and models for the management of information security (Lee et al. 2016; Silic and Back 2014). It is typical to operationalize information security management as frameworks (Siponen and Willison 2009), including maturity models (Almuhammadi and Alsaleh 2017). These models, especially the popular information security management standard ISO27001, date back to times before the emergence of Zero Trust (Backhouse et al. 2006), and thus, do not incorporate the foundational principles of Zero Trust; defense is built around the perimeter that seeks to keep the "enemy at the gate" (Whitman 2003). Given that organizations are still lagging in their Zero Trust adoption (Buck et al. 2021; Lacity and Carmel 2022), maturity models seem particularly appealing as they enable organizations to gradually climb the maturity ladders rather than having to approach Zero Trust through big bang implementation. Next, we review the existing Zero Trust frameworks, maturity models in the context of information security management and the socio-technical perspective.

Zero Trust

While the concept of Zero Trust is a hot area that has gained traction only recently (Lacity and Carmel 2022), its foundational idea can be traced back to the origins of the internet as documented in the RFC 1122 standard from 1989: “In general, it is best to assume that the network is filled with malevolent entities that will send in packets designed to have the worst possible effect” (Braden 1989). For a long time, this principle was only seen to relate to the untrusted “external” or “public” network (Internet) rather than to the trusted “internal” and “private” (Intranet) (Kindervag et al. 2016). Zero Trust seeks to eliminate this idea of trusted and untrusted networks and rather posits that “there is no sense of a safe perimeter where devices or users are trusted a priori.” (Lacity and Carmel 2022, p. 244) Microsoft formulated three principles for Zero Trust:

1. **Verify Explicitly:** Organizations that verify explicitly use all data and information available to reduce uncertainty and implicit trust.
2. **Use Least Privileged Access:** Using the least privilege is always providing the least number of permissions necessary.
3. **Assume Breach:** Assuming breach is when you already consider your digital environment compromised.

While research on the topic is still lagging, the implications of these principles may be dramatic not only for information security but for societies as a whole. For instance, recent research from Vuorinen and Uusitupa (2022) found that the Zero Trust model, when compared with the traditional perimeter security, induces a shift in the “ethos” (“the central characteristics of security model through which its subjects – security, user, and organization – are constituted” (p. 52)) of information security. According to the authors, this shift implies a fundamental transformation from “societies of discipline”, as the ethos of perimeter security, into “societies of control” as the new ethos of Zero Trust.

While it is possible to build a security strategy based on Zero Trust, the model traditionally only addresses the weakness of implicit trust in a communications network (Lacity and Carmel 2022). Because of this, some security researchers have called this approach to security architecture fundamentally flawed (SABSA 2019). Multiple maturity models have been proposed with the purpose to help organizations assess and improve their Zero Trust capabilities, but these models tend to focus on technical aspects of information security and are either developed by government organizations or for commercial purposes. Thus, their application to non-government organizations and vendor-independent contexts can be challenging. Several of these models seek to promote their own proprietary Zero Trust solutions within the company’s eco-system. Information systems security scholars have remained largely mute about the topic, and academic research on the topic, in general, is lagging behind (Buck et al. 2021) leaving practitioners without their much-needed guidance.

One of the notable exceptions of Zero Trust research approaching security holistically is from Modderkolk (2018) who designed a maturity model for assessing organizational and technical aspects of information security maturity with Zero Trust as the focal point. However, while the model includes the principles of Zero Trust, it only limits the application of those principles to the technical aspects and does apply them to other domains of information security. As such, his model is a kind of hybrid combining Zero Trust and traditional principles with technical and social aspects respectively. Other relevant models mainly focus on technology (see Table 2). Building an overall information security strategy based on such models is challenging as they do not address organizational aspects such as processes and people. This is supported by Soomro et al. (2016) who highlight the importance of access control, defining security policies, security awareness, and training and argue that a holistic approach is necessary for information security management. As May & Dhillon (2010) argue, information security has become a multidimensional discipline where both social and technical considerations must be considered in a coherent manner.

Maturity Models

Maturity models are used to assess organizations’ as-is situation of current capabilities in a certain domain against predefined maturity levels. Further use includes prioritizing future improvements and measuring progress (Pöppelbuß and Röglinger 2011). Different levels are used to describe a path from the initial state to improved maturity of capabilities (Becker et al. 2009). According to Gottschalk & Solli-Sæther (2009) “some models suggest that organizations progress through stages while others argue that there may be multiple paths through the stages” (p. 110). The maturity models provide organizations with tools that can be used as the basis for assessment and improvement. Software Engineering Institute (SEI) published the "Capability Maturity Model for Software" in 1993 (Paulk et al. 1993). The model has served as a blueprint for a large number of other maturity models developed since then (Pöppelbuß et al. 2011). This has led to maturity models being the subject of criticism due to their perceived redundancy (Becker et al. 2009). Other points of criticism have been the lack of documentation of the design process and principles used during development (Pöppelbuß et al. 2011).

de Bruin et al. (2005) suggest three different application-specific purposes for maturity models: descriptive, prescriptive, and comparative. Models that are descriptive are purely used to describe the as-is and do not make any suggestions to improve maturity. Prescriptive models are used by organizations to improve their capabilities, while comparative models can be used to compare practices across industries and industry standards.

Maturity Models for Information Security

There are several maturity models for information security, some of which take a general approach while others focus specifically on Zero Trust. We compared four prominent maturity models in this paper, two general models and two Zero Trust models: The Cybersecurity Capability Maturity Model (C2M2) focuses on overall cybersecurity posture, while the capability maturity model aims at assessing the maturity of Security Operation Centers (SOCs) based on the use of Cyber Threat Intelligence (CTI) (CTI-SOC2M2) focuses on SOC and CTI integration. Two Zero Trust Maturity Models focus on technical aspects of Zero Trust implementation. There are also other maturity models in the information security area (Almuhammadi and Alsaleh 2017; Chouikh et al. 2023; Saleh 2011), but due to space limitations, we review only these four focusing on Zero Trust.

The C2M2 was developed by the U.S. Department of Energy in collaboration with the U.S. Department of Homeland Security and subject-matter-experts from the electricity subsector (Office of Cybersecurity, Energy Security, and Emergency Response 2021). C2M2 aims to help organizations build better cybersecurity programs, benchmark capabilities, and prioritize future actions and investments. C2M2 has four different stages of maturity, ranging from zero to three. The model includes control questions to evaluate maturity in 10 different domains within information security. Maturity within domains is independent of each other.

Instead of providing a maturity model to assess overall cybersecurity in an organization, the CTI-SOC2M2 model focuses on one very specific domain (Schlette et al. 2021). It aims to improve the integration between CTI and SOC. It does so by mapping CTI data in different formats to services often provided by SOC. Six different levels are used to rank the ability to integrate each CTI format into different SOC services. An overall maturity level is then evaluated based on capabilities within each service. The overall maturity level is divided into four stages – Initial, core, extended, and visionary. The highest level of maturity is achieved when capability level four is reached for all services.

Zero Trust Maturity Model (ZeTuMM) was developed by Modderkolk (2018). It is a model for assessing organizations' cybersecurity capabilities according to the Zero Trust principles. Zero Trust is only present for areas related to technology, while organizational areas are based on best practices identified in other frameworks and models. The model ranks maturity on three different levels. 53 capabilities are hosted within 15 domains (referred to as focus areas). 428 control questions are listed and used to determine maturity. Controls suggested within the model have been derived from established frameworks such as CIS Controls and the NIST Special Publication 800-53.

The CISA Zero Trust Maturity Model (ZTMM) was developed by The Cybersecurity and Infrastructure Security Agency (CISA) and suggests a path for organizations to transition to Zero Trust (CISA 2021). While the model aims to provide a holistic approach to adopting Zero Trust it is still very technology-focused. Even though it extends beyond network-centric applications, it lacks the adaptation of Zero Trust principles on processes and other organizational aspects. Five domains are used to cover the areas to be assessed. The included domains are Identity, Device, Network/Environment, Application Workload, and Data. Capabilities related to the categories "Visibility and analytics", "Automation and orchestration", and "Governance" are suggested for each of the five domains. Maturity is measured in three stages – traditional, advanced, and optimal. A summary of the four maturity models can be found in Table 1.

Requirement	C2M2	CTI-SOC2M2	ZeTuMM	CISA ZTMM
Design Process	Initial draft developed by industry advisory group. Second draft is based on expert feedback.	Maturity model comparison and literature study	Maturity model comparison, literature study, and case study validation	N/A
Content	General information security capabilities	The specific domain within information security (CTI and SOC services)	General information security capabilities with Zero Trust as the focal point	Information security capabilities related to Zero trust. Technology focused

Table 1. Maturity Model Comparison

The table below (Table 2) lists the topics addressed by the four maturity models. T means that the model addresses the topic with recommendations from traditional best practices. ZT means that the model recommends an approach based on Zero Trust principles. Focus Areas listed in the table do not necessarily correspond directly to the domains/structure of any given model in the same table.

Focus Area/Model	C2M2	CTI-SOC2M2	ZeTuMM	CISA ZTMM
Asset, Change and Configuration Management	T			ZT
Threat and Vulnerability Management	T	T	ZT	
Risk Management	T		T	
Identity and Access Management	T		ZT	ZT
Situational Awareness	T			
Event & log management	T	T	ZT	
Incident response, continuity of operations	T	T	T	
Third party risk management	T			
Workforce management	T		T	
Cybersecurity architecture	T		ZT	ZT
Cybersecurity Program Management	T			
Security Monitoring, Analysis & Threat Detection	T	T	ZT	ZT
Cyber Threat Intelligence Sharing		T		
Threat Hunting, Penetration Testing & Digital Forensics		T		
Lifecycle management: IT, data, IS	T		T	ZT

Table 2. Comparison of existing maturity models.

This maturity model review illustrates the lack of a holistic maturity model that incorporates Zero Trust in technical as well as organizational aspects of information security.

Socio-Technical Perspective

Socio-technical perspective is well-established within the IS research and is even considered the "axis of cohesion" within the otherwise topically and theoretically fragmented discipline (Sarker et al. 2019). A key tenet of the socio-technical perspective is the idea that any changes in the technological system will imply changes in the social system and vice versa (e.g., Mumford 2006). Thus, efforts should focus on their joint optimization (Bostrom and Heinen 1977) but also on their fit and harmony (Sarker et al. 2019). Socio-technical perspective also includes strong humanistic objectives (in addition to instrumental, i.e., joint optimization) that emphasize quality of work life and justness (Sarker et al. 2019). Zero Trust's focus on replacing trust with verification may amplify the importance of these humanistic objectives (Vuorinen and Uusitupa 2022).

When the socio-technical perspective is applied to the information security context, information security becomes an outcome, even if often the contingent outcome, of the joint optimization between the social and the technical (Coles-Kemp 2009). In other words, the socio-technical perspective does not prioritize the social or the technical over one another. Consequently, the socio-technical perspective questions the view that any security event could be simply labeled as "human error" (or "technology failure") and, instead, requires unpacking any such event as the joint outcome between the human and the technological aspects. To put it more concretely, in any security incident of "human error", there is also likely some related weakness in the technology. This view of socio-technical relates well to what Vuorinen and Uusitupa (2022) argue: "*At the theoretical level, Zero Trust Model cannot blame the user as it does not trust the user in the first place*. It authenticates the user not by the essence of a user (what user is) but through user's effects on other actors i.e., in what way the user uses the network." (p. 59, emphasis theirs). Last, socio-technical view, by emphasizing the social and the technical evenly, provides a theoretical basis to respond to calls on "holistic" information security management. From the socio-technical perspective, information security management is founded on the joint development of the social, e.g., organizational processes and people, and the technical, e.g., security technologies (Eloff & Eloff, 2005).

Design Science Research Approach

Design science research (DSR) was used as an approach to design a maturity model as an improved framework (Baskerville et al. 2018; Gregor and Hevner 2013) with which organizations can evaluate their organizational Zero Trust maturity and use it as a basis to develop their information security. The design of the artifact was motivated by the practical need to address organizational information security holistically, which requires extending Zero Trust from the technical aspects to the organizational aspects. This practical need was first noticed as some of the authors worked as information security consultants and architects. They could not find the necessary tools to support their security consulting work, which was a concern that resonated well also among their colleagues. The authors worked with several businesses of varying information security maturity, and the businesses all had one issue in common: finding an easily understandable framework that guided them on their Zero Trust journey while also addressing information security holistically. As a result, a collaborative project with researchers was initiated to design an artifact for practical needs. The design took place between September 2021 – May 2022.

To generate the initial descriptive knowledge base for the design of the artifact, a literature review was conducted with the purpose of uncovering the current academic and practical knowledge on Zero Trust and on maturity models (Gregor and Hevner 2013). In section 2, we present the key aspects of the results of the literature review as a knowledge base for the artifact. Following Hevner et al. (2004), the design environment of EZTMM is in Figure 1.

The artifact was developed through three phases: 1) problem awareness and design suggestions, 2) three development iterations, and 3) an evaluation phase (Kuechler and Vaishnavi 2008), which we describe in the following section. A key objective of the design was to develop a holistic model for Zero Trust even if models on the technical aspects already exist. Focusing only on the social aspects would have violated the socio-technical foundations of the approach. During each phase, the maturity model was developed by the authors along with information security experts from six different organizations that served as informants for the design project. Although most experts were working for large companies, several experts were working as security managers for small or medium-sized businesses, while being employed in a larger consulting company. Many experts also had prior experience working in small to medium-sized businesses.

The experts were from various sectors including the process industry, information security consulting, finance, and the food industry. Our informants had extensive 5-30 years of experience working within the field of information security and were recruited to take part in the process based on their known level of expertise in the substance area. The informants had different organizational roles: Chief Information Security Officer (3 informants), security manager (4), and technical specialist (2).

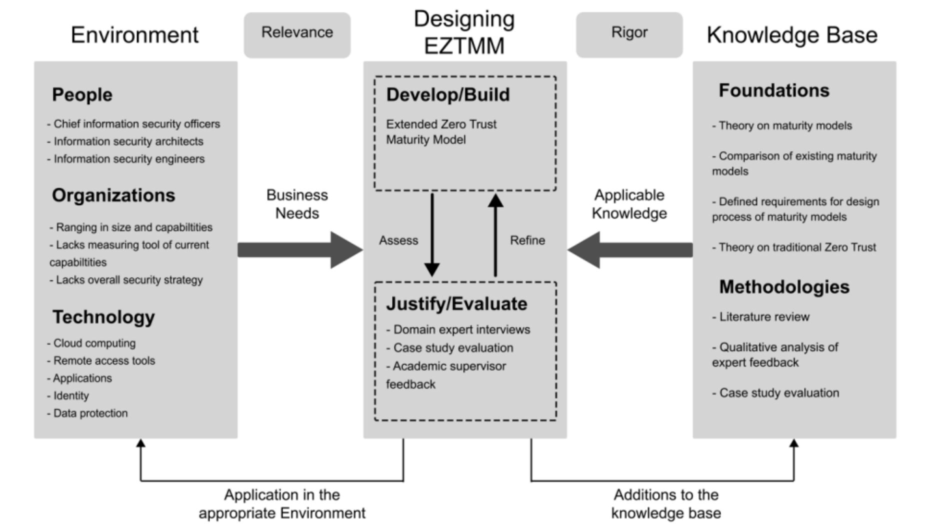

Environment
Relevance
Designing EZTMM
Rigor
Knowledge Base
People
- Chief information security officers
- Information security architects
- Information security engineers
Organizations
- Ranging in size and capabiltities
- Lacks measuring tool of current capabiltities
- Lacks overall security strategy
Technology
- Cloud computing
- Remote access tools
- Applications
- Identity
- Data protection
Business Needs
Develop/Build
Extended Zero Trust Maturity Model
Assess
Refine
Justify/Evaluate
- Domain expert interviews
- Case study evaluation
- Academic supervisor feedback
Applicable Knowledge
Foundations
- Theory on maturity models
- Comparison of existing maturity models
- Defined requirements for design process of maturity models
- Theory on traditional Zero Trust
Methodologies
- Literature review
- Qualitative analysis of expert feedback
- Case study evaluation
Application in the appropriate Environment
Additions to the knowledge base

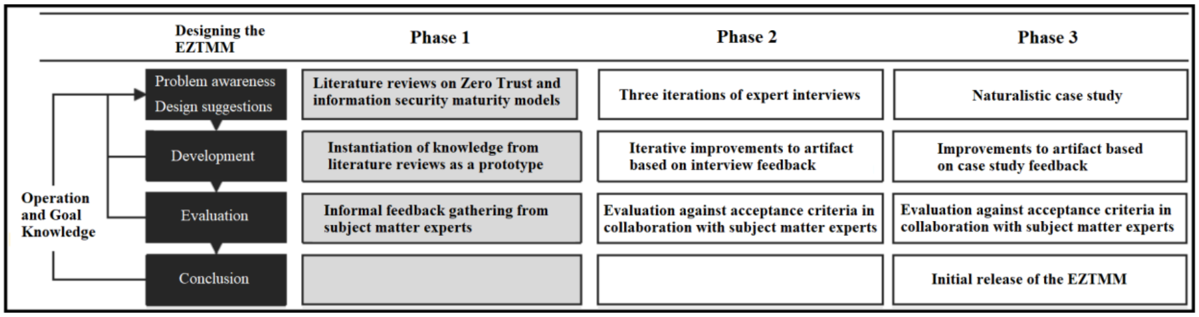
Figure 1. Designing the EZTMM

After the completion of each development iteration, we had to decide if the model was to be considered finalized or whether, yet another iteration was required (formative evaluation in (Venable et al. 2016)). To help with the decision, for each iteration, the informants (subject matter experts and practitioners) were asked if the model was satisfactory in terms of overall quality, usability, and efficiency. We also asked for additional feedback and if they saw any need for further changes.

When a consensus of satisfactory quality was reached among the informants, and no further major changes were imposed, the final evaluation could start. This phase involved a naturalistic and summative case study, where the model was tested in an informant organization (Venable et al. 2016). The participants in the organization carried out the assessment on their own, while two of the researchers observed and took notes on how the model was used. These observations, as well as feedback from the informant performing the assessment, provided data to improve the model even further. After the case study evaluation, we deemed the model to be ready for publication while acknowledging that further design iterations might be needed in the future as more experience accumulates in its use in practice.

Designing the Extended Zero Trust Maturity Model

In this section, we will describe the process used when designing the Extended Zero Trust Maturity Model (EZTMM). The design process was performed in three phases: problem awareness (including the literature review and existing model comparison), development (the initial interviews, the second interviews, and expert feedback), and the evaluation with a case study. An overview of the phases can be found in the figure below (Figure 2), and each phase is described in detail in the following chapters to increase the transparency of the design science research (Järveläinen et al. 2022). Figure 2 depicts the design process structured along the steps of DSR (Kuechler and Vaishnavi 2008). The process is presented in a rather linear form due to readability while the actual process was cyclic. For instance, while the most effort in reading and reviewing literature was done at the very beginning of the design process, reading literature continued throughout the whole process.



Designing the EZTMM	Phase 1	Phase 2	Phase 3
Problem awareness Design suggestions	Literature reviews on Zero Trust and information security maturity models	Three iterations of expert interviews	Naturalistic case study
Development	Instantiation of knowledge from literature reviews as a prototype	Iterative improvements to artifact based on interview feedback	Improvements to artifact based on case study feedback
Evaluation	Informal feedback gathering from subject matter experts	Evaluation against acceptance criteria in collaboration with subject matter experts	Evaluation against acceptance criteria in collaboration with subject matter experts
Conclusion			Initial release of the EZTMM

Figure 2. EZTMM Phases Overview

Problem awareness and a design suggestion: Reviewing the knowledge base and building the first draft on Zero Trust

The foundation of the EZTMM was formed through a literature review conducted in the Autumn 2021. In this literature review, we identified the core concepts of a Zero Trust architecture and compared existing Zero Trust maturity models. During this work, we found that Zero Trust principles are mainly applied to the technology domain in these maturity models (see Table 2). This review confirmed our experiences as practitioners with the need of extending Zero Trust to organizational information security in order to create a more holistic maturity model, i.e., to consider an organization's processes and people, as well as its technology (Eloff & Eloff, 2005).

Based on the initial findings from the literature review, we started developing a qualitative interview guide in parallel (Myers and Newman 2007). We started by organizing pilot interviews in November 2021 to gather feedback on the interview guide and gain further insight into Zero Trust concepts. These interviews were conducted during the first iteration to collect knowledge from the expert informants.

We then crafted an initial design suggestion for the model building on the core concepts of Zero Trust that we identified through a literature review and the prior literature on maturity models. The core Zero Trust principles were applied to organizational aspects of information security that were not traditionally associated with Zero Trust. This was our first attempt at creating a more holistic Zero Trust maturity model. The result of this work was compared against prominent security frameworks and models such as ISO 27001, national information security guidelines, and Center for Internet Security (CIS) Controls. The goal of this comparison was to identify gaps in our own maturity model and get an understanding of existing security controls. Based on this, we defined three maturity levels for each focus area, along with control questions the organization can use to assess their current maturity level. In other words, the initial model and the control questions resulted from a dialogical reading of the prominent (non-Zero Trust, perimeter-based) frameworks and the principles of Zero Trust. This meant explicitly confronting the existing "best practices" as documented in these existing frameworks with the Zero Trust principles in an attempt to understand their implications. The maturity levels were inspired by the levels defined by CISA in their Zero Trust Maturity Model (CISA 2021). Simultaneously to our dialogical reading, we sought for early feedback and evaluation (Vom Brocke et al. 2020) for the emerging and model and accompanied control questions from practitioners working in the same company as some of the authors. These experts were deemed valuable sources for early feedback due to their availability but also due to their broad and deep knowledge as experienced information security consultants. This resulted in our initial draft of the EZTMM including a total of 72 control questions within 10 focus areas.

Development of the artifact

First iteration: Restructuring the initial EZTMM draft jointly with experts

The initial draft was then sent out for review to our informant organizations. A total of six informants from five different organizations were included in the first feedback round. All the informants were security professionals, ranging from technical specialists and engineers to managers and chief information security officers (CISOs). The goal of this iteration was to improve all aspects of our model, including restructuring the model, adding new focus areas, and rearranging maturity level requirements and control questions.

After a two-week review period, we received written feedback on our initial draft and arranged one-hour interviews with all the informants following a semi-structured interview guide to obtain more feedback. The interview guide included questions on Zero Trust model in general, EZTMM contents, structure and use. We also arranged a presentation and workshop in one of our informant organizations with over ten security professionals. During the workshop, we presented the topic of Zero Trust while introducing our initial maturity model draft and gathering feedback.

The feedback on the initial draft could generally be classified into three categories: 1) Focus Area Improvements and Suggestions, 2) Corrections and Consistency, and 3) Structure Improvements. All feedback gained in every iteration was categorized and prioritized by the authors using a review table including a column for each of the above mentioned categories. Decisions were made in consensus on whether to implement the feedback or not. A change log of implemented changes from each version of the EZTMM was kept, along with the table of categorized feedback, containing our decision on whether to implement it and the reasoning behind the decision.

The first type of feedback was new focus area suggestions: "*Emphasize backup and restore further in the model. Perhaps in their own focus area? Immutable backups are Zero Trust principles being applied to backups." (CISO 1).* In this case, we decided that an increased emphasis on backups in the Data Governance Focus Area would be sufficient. We received similar comments on out-of-band-communications: *"How about collaboration tools? If an attacker has compromised your AD [Active Directory], how do you communicate? Perhaps establishing out-of-band collaboration solutions." (CISO 2).* Similarly, to the first suggestion, this topic was included and emphasized in our existing Incident Management Focus Area.

Corrections were also common, especially among the technical specialists. These were generally minor corrections such as "*Add also VRFs [Virtual Routing and Forwarding]. VRFs play a key role at route-segmentation level.*" (Technical specialist 1), most of which were implemented. There were also comments related to the consistency of the writing, all of which were implemented: "*Consider the style in which the maturity levels are defined. In many requirements, the text describes what an organization "should" do to reach a specific maturity. Some maturity models would describe what an organization "is" doing when they are at a specific level." (CISO 2)*

Lastly, we received a lot of comments regarding the structure of the model. Many informants commented that they struggled to see the connections between our focus areas: "*When I read these focus areas, I see a good mix without seeing the connection between them*". (Security Manager 3) Based on this feedback, we restructured our model by adding three domains: Technology, Processes, and People (see also Eloff & Eloff, 2005). These domains allowed us to easily categorize each focus area and highlight the importance of a holistic approach to Zero Trust.

During iteration 1, we made a lot of significant changes: We restructured the model and introduced the three domains. We also implemented several corrections, improved the consistency of the writing, and put more emphasis on important topics such as backups, using a risk-based approach and out-of-band communications. The result of implementing the feedback from our informants was the second draft of the Extended Zero Trust Maturity Model. The second draft of the EZTMM included a total of 85 control questions within 10 focus areas and three domains. 13 new control questions were added, and three questions were revised based on informant feedback.

Second Iteration: Further development of the second draft of EZTMM with experts

The second draft of our maturity model was then sent out to all the informants from the previous round of feedback as well as three new informants from three new organizations. Any changes made from the initial draft were marked yellow and allowing us to decrease the review window to one week. The goal of this iteration was to improve and polish most aspects of the model, making sure everything was clear and correct without making large changes.

After receiving written feedback on the second draft, we scheduled follow-up interviews with each informant. The informants were asked to provide further written feedback if any came to mind at the end of the interview. Most of them provided some additional feedback. The suggestions collected from the written feedback and follow-up interviews were inserted as comments and evaluated using the same process as described in iteration 1.

There were three recurring themes in the iteration 2 feedback: 1) insufficient coverage of identities, 2) negative experiences with phishing simulation tools, and 3) insufficient focus on the Zero Trust principles in the focus areas under the people domain.

The lack of focus on identity in our framework was pointed out by multiple informants:

"*I miss a bit more about IAM [Identity and Access Management] here? Maybe particularly identity governance and tying authentication to other tools such as EDR [Endpoint Detection and Response] and MDM [Mobile Device Management]?"* (Security Manager 1) Due to this feedback, we decided to add a new focus area dedicated to the governance of identities: Identity and Access Management. Furthermore, we rewrote the Dynamic Access section under technology to emphasize more clearly how identities are used to determine access.

Several of the informants this time around also had bad experiences with phishing simulation tools: "*I have strong opinions about the "usefulness" of these tools…reach out if you want to hear why I mean they are indeed useless if not even damaging the security culture of an organization."* (CISO 1) Based on our informants' negative experiences with the tools, we decided to do further research on the topic. As a result, phishing simulators were removed as a maturity level requirement in our model based on recent findings that suggest such tools can have negative impacts (Lain et al. 2022).

Lastly, the focus areas in the people domain were rewritten, increasing the emphasis on Zero Trust principles. This was done to address comments such as: "*Where is zero trust here? What you describe makes sense also in terms of maturity level, but where is the "assuming compromise" or other "ideas" of zero trust?*" (CISO 2) The result of this process is the third draft of the EZTMM, which included a total of 104 control questions within 11 focus areas and three domains. 19 new control questions were added and 13 were revised based on informant feedback.

Third Iteration: Expert Feedback on Identity

To ensure the quality of the newly added focus area, we performed an additional short iteration, where we asked two of our subject matter experts for written feedback on the new focus area and the rewritten dynamic access area in particular.

The feedback was positive overall, validating that we had captured the essence of identity in Zero Trust. In addition to receiving formal acceptance for the newly added and rewritten focus areas, we received some minor additions along with some corrections and comments on the consistency of the writing: "*Mention something about assigning rights based on the role extracted from the HR system*" (Technical specialist 2) and "*Be consistent…either short version first and then explanation…or the opposite…as you have it for CSF [Critical Success Factor]*" (CISO 2). These comments were addressed and implemented to EZTMM, prior to conducting the case study evaluation. Over the course of all three iterations, we received a total of 51 corrections and consistency, 20 structure, and 28 focus area suggestions.

Naturalistic case study evaluation

In the third phase, we conducted a case study evaluation of our maturity model to evaluate its utility (Hevner et al., 2004). We asked one of our informant organizations to perform a maturity review using our model while one of the authors was present to take notes but also to support them on the use of the model should there be a need. The organization is one of Norway's largest publicly traded organizations. The evaluation was performed in May 2022 by the organization's IT architecture department with assistance from other relevant departments when needed. Answering the questions requires input from a range of stakeholders in the organization including human resources and business units among others. We were tightly involved in the maturity review process, gathering data on how the model was used as well as direct feedback from the people using it to assess their organization's maturity.

To guide the evaluation effort, we formulated evaluation goals (Venable et al. 2016). With the naturalistic, summative evaluation, the artifact effectiveness was tested in a real situation (Venable et al. 2016). In the naturalistic case study evaluation, the model was compared against the acceptance criteria listed in Table 3 below. These requirements evolved throughout the research, in accordance with the growing knowledge base, especially the general design principles for maturity models developed by Pöppelbuß & Röglinger (2011). The requirements in the table are the total requirements, including both the informant acceptance requirements after each iteration and the other requirements tested during the case study.

After the evaluation had been performed, we interviewed the person who conducted the maturity assessment about the use of the spreadsheet and recorded the answers. The interview focused on questions derived from the evaluation goals (see Table 3). For instance, we asked if the supporting documentation was sufficient to provide an answer to the control questions in order to get informants view on the evaluation goal “Can be used to self-assess the current Zero Trust maturity”. These interview responses complemented our own observation notes from the evaluation.

Evaluation Goal	**Rationale**
Applicable in a broad range of organizations	For a maturity model to be adopted and considered useful by organizations, it needs to be applicable. Therefore, a broadly applicable model is a prerequisite for broad adoption.
Can be used to self-assess the current Zero Trust Maturity	The main purpose of our maturity model is that it can be used for assessing organizations’ Zero Trust maturity level.
Can be used to improve overall information security capabilities	An important use for maturity models is to assess the organization’s maturity and based on this assessment identify improvements, and low-hanging fruits and plan further implementation. The model, therefore, needs to be able to facilitate this.
Applies Zero Trust principles holistically to both technical and organizational domains within information security	The main knowledge gap identified in our literature review was that existing models do not take organizational domains sufficiently into account. This model was intended as a possible solution.
Security controls suggested in the model are placed at appropriate levels and described sufficiently and correctly	The model’s usefulness depends on it being correct. Controls placed at the wrong level lowers the usability and credibility of the model.
Informants being presented with the model show a desire to leverage the model in their own organization	Informants showing interest in using the model give an indication of the relevance and potential value provided by the research.
Informants have few or no additional suggestions for changes when being presented with the latest draft of the model.	Receiving a few suggestions for changes indicates that consensus is reached among the informants and that the model has reached an acceptable level of correctness.

Table 3. Evaluation goals for the EZTMM

The evaluation was done using our EZTMM Evaluation Sheet (see Figure 3 for the overview dashboard). This spreadsheet was developed as an evaluation tool based on the EZTMM and includes every control question introduced in the model in a color-coded format based on which domain the question belongs to.

Most of the feedback was related to specific questions in our model, such as “*Is it possible to split this into multiple questions? We use asset management tools, but do not have a fully implemented CMDB [Configuration Management Data Base]?*” (Security Manager 1) These comments were addressed, resulting in a revision of several control questions. We also received requests for clarification: “*This point is poorly explained, could perhaps have been elaborated on in the document.*” (Technical Specialist 2). These requests were also addressed, leading to further additions to the descriptions of some maturity levels in the EZTMM.

Lastly, we received some comments on the maturity assessment spreadsheet itself. One such comment was that the dashboard could have been more detailed. "*Would possibly have been useful to have some additional details in the dashboard for when the sheet has been filled out*." (CISO 3) We addressed this comment by increasing visibility into the scoring on each maturity level for each focus area. Several corrections were also made to the spreadsheet, such as the Data Governance and Protection initially being incorrectly placed in the Technology domain in the original model and the maturity level calculations of every subsequent focus area being incorrectly calculated as a result.

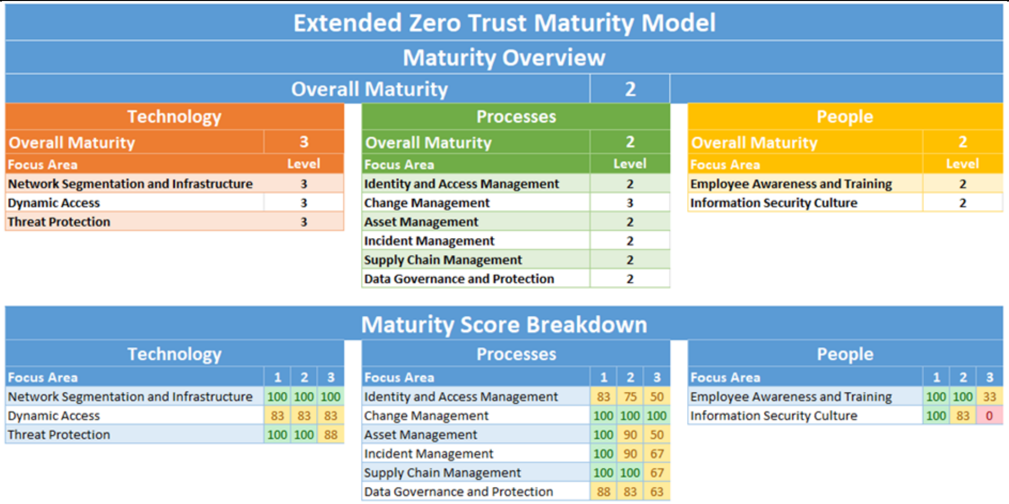
The only improvement suggestion we were unable to implement due to a lack of time was weighted focus areas:

> *"It is a good tool for providing a snapshot of where an organization is and the competency that is there. However, I think it was difficult to determine in which end to start and how to prioritize improvements." (Security Manager 4)*

Implementing this suggestion would require a lot of additional research into how to correctly weigh the focus areas relative to each other. We decided that this would not be possible given the time constraints for the research. Implementing the feedback from the case study evaluation resulted in a total of 107 control questions within 11 focus areas and three domains. Three new control questions were added and eight were revised based on informant feedback. The result of these changes was V1.0 of the EZTMM, our first release version.

The Extended Zero Trust Maturity Model

The final artifact consists of a spreadsheet and a text document. The spreadsheet contains usage instructions, 107 control questions across all three domains and 11 focus areas, and a dashboard that can be used for both reporting and gaining an overview of the current status. The spreadsheet is designed in such a way that it can be used by both technicians, reviewing and answering specific control questions and management for reporting on the overall maturity and progress in each focus area. Storing the control questions and accompanying comments in the same spreadsheet used for reporting makes it simpler to drill down and investigate the root cause of a certain maturity level not being achieved in any focus area or domain. It also promotes discussion and cooperation between upper management, security managers, and technicians. It does this while giving a good overview of the situation and helping translate technical terms into a more understandable format for reporting and compliance purposes.



Extended Zero Trust Maturity Model

Maturity Overview

Overall Maturity 2

Technology

Overall Maturity	3
Focus Area	Level
Network Segmentation and Infrastructure	3
Dynamic Access	3
Threat Protection	3

Processes

Overall Maturity	2
Focus Area	Level
Identity and Access Management	2
Change Management	3
Asset Management	2
Incident Management	2
Supply Chain Management	2
Data Governance and Protection	2

People

Overall Maturity	2
Focus Area	Level
Employee Awareness and Training	2
Information Security Culture	2

Maturity Score Breakdown

Technology

Focus Area	1	2	3
Network Segmentation and Infrastructure	100	100	100
Dynamic Access	83	83	83
Threat Protection	100	100	88

Processes

Focus Area	1	2	3
Identity and Access Management	83	75	50
Change Management	100	100	100
Asset Management	100	90	50
Incident Management	100	90	67
Supply Chain Management	100	100	67
Data Governance and Protection	88	83	63

People

Focus Area	1	2	3
Employee Awareness and Training	100	100	33
Information Security Culture	100	83	0

Figure 3. EZTMM Maturity Dashboard

The text document contains further information on all 11 focus areas and accompanying control questions. Each focus area has a short description of that focus area itself and its importance, more detailed descriptions of each maturity level, an overview of each maturity level in a table format, and the control questions. Figure 3 below shows the EZTMM maturity dashboard from the spreadsheet. It illustrates the structure of the EZTMM, with all of its three domains and 11 focus areas. The maturity evaluation is based on the answers provided for the 107 control questions detailed in the EZTMM. A score of at least 75 for each maturity level in a given area is recommended before moving on to the next level. This, along with the partial implementation of a measure awarding half score for any given question, is to allow businesses more flexibility in which assets they chose to protect based on criticality and other criteria specific to their organization. Further samples of the EZTMM evaluation spreadsheet and the model itself were cut due to space constraints [1].This model was designed to assist organizations on their Zero Trust journey by giving concrete examples of applying the core principles of Zero Trust not only to the technological aspect but also to the organizational aspects covering people and processes. By exemplifying how this can be done, the model not only provides guidelines and concrete measures an organization can implement, but it also encourages organizations to apply Zero Trust principles broadly, creating their own controls based on the same core principles.

Discussion

In this research, we have designed a holistic maturity model we coined as EZTMM that extends the principles of Zero Trust from purely technological aspects to the organizational aspects of information security that include people and processes. In our comparison of existing maturity models, we discovered a gap in models created for assessing Zero Trust maturity where none focused on applying the socio-technical approach to Zero Trust. Further, our review of the central IS management maturity models suggested that none of the models applies Zero Trust principles. We have addressed this gap by designing a maturity model that builds on the Zero Trust principles and addresses both the technological and organizational side of information security. Our research contributes to the need for holistic information security approaches (May and Dhillon 2010; Soomro et al. 2016) and to calls to reconsider foundational assumptions of IS security (Lowry et al. 2017).

By building on the socio-technical ideas (Mumford 2006; Sarker et al. 2019), EZTMM extends the principles of Zero Trust from the technical to the organizational aspect. This extension makes a novel contribution to design knowledge (Gregor and Hevner 2013) and to the literature on information security management (e.g., Dlamini et al. 2009; Soomro et al. 2016). To the best of our knowledge, the designed artifact is the first maturity model that seeks to expand the principles of Zero Trust to the “social” domain, to the people and processes. The designed artifact can be readily used by organizations as illustrated by the case study evaluation. Further, the designed artifact fulfills the formulated design goals (Venable et al. 2016) and its utility has been demonstrated through a case study (Hevner et al., 2004). However, this does not mean that the designed model should replace or overthrow other existing models. Indeed, some models have a much narrower scope and may thus be more helpful in a specific context. For instance, CTI-SOC2M2 model focuses specifically on security operations centers that are very specific in context. In contrast EZTMM, seeks to address the needs of “all” organizations. We highlight the contributions of EZTMM to information security maturity models in Table 4.

Focus Area/Model	Contributions of EZTMM
Asset Management	EZTMM extends traditional, best practice-based C2M2 and extends CISA ZTMM with Zero Trust principles.
Change Management	EZTMM extends traditional, best practice-based C2M2 and extends CISA ZTMM with Zero Trust principles.
Identity and Access Management	EZTMM extends traditional, best practice-based C2M2 and complements ZeTuMM and CISA ZTMM with Zero Trust principles.

[1] The EZTMM can be found here: https://drive.google.com/drive/folders/1vPbMb_Xox62iLhgHZ1jpoWUi68c2cadR?usp=sharing

Incident response, continuity of operations	EZTMM extends traditional, best practice-based maturity models by incorporating Zero Trust principles.
Supply Chain Management	A novel focus area for the application of Zero Trust principles
Data Governance and Protection	A novel focus area for the application of Zero Trust principles
Employee Awareness and Training	A novel focus area for the application of Zero Trust principles
Information Security Culture	A novel focus area for the application of Zero Trust principles

Table 4. The contributions of EZTMM to information security maturity models.

The designed model was initiated by practical need (Gregor and Hevner 2013), and it contributes to fulfilling this need. While all practitioners involved were from the same country, they represent significant domain-specific expertise and several different companies. Further, some of our informants work in consultation roles that have afforded them to see several different environments and the needs of those environments. As such, we expect that the model can make a significant contribution to the practice of information security management and contribute to a broad audience of security practitioners beyond those who participated in the process. Nevertheless, more research is needed to learn about the boundaries and limitations of the application of the model in maturity evaluations.

A key aspect of the EZTMM is the adoption of Zero Trust principles to organizational aspects of information security which importantly challenges existing design assumptions and foundational principles in information security management (Lowry et al. 2017). The more technologically-minded practitioners have already taken use of the Zero Trust principles to advocate approaches to, e.g., access control and network security (e.g. Ahmed and Petrova 2020), but have remained largely mute on the broader application of these principles (Buck et al. 2021). In this research, we have shown that it is possible to design a model that builds on the Zero Trust principles and extends these principles beyond the technical domain. Based on the expert evaluations during the design process, extending the Zero Trust to organizational aspects was well taken. Applying these principles to the organizational aspects changes the well-trodden metaphor of the organization as a fortress (e.g., as traditionally practiced) into a metaphor of organization like a public market square where it is never known who might be pickpocketing or posing other types of threats. Such requires removing much of the implicit trust even within the organization and its premises. But is such ever attainable inside an organization, and if, yes, what could be its consequences for organizing? After all, the majority of human life, whether it is inside or outside of organizations, rests on trust (McKnight et al. 1998; Slovic 1993). Indeed, this is one of the key challenges we have confronted when designing the artifact and extending the Zero Trust principles to the organizational aspects. How much of the inherent trust within an organization can be reduced before it starts interfering with more significant organizational goals? We expect that the answer to this is context dependent where some organizations and functions may be able to operate with less trust whereas others require more trust between employees, e.g., military organizations contra start-ups.

During the artifact evaluation, we used the EZTMM as a tool to evaluate the maturity level of an organization but lack knowledge on the implications of its use as a development tool. Such cases will be crucial and help to determine the applicability of the designed model across contexts, but they should be implemented and analyzed with care to not promote an organizational culture where healthy skepticism is replaced with a potentially crippling "suspect everyone" attitude. Information security professionals, however, are likely well-equipped to deal with tensions (Niemimaa & Niemimaa, 2019; Soliman & Ojalainen, 2023) as they have done other similar tensions of security vs privacy, security vs usability and so on.

Given the above, this research makes an important contribution to the literature on information security management. Information security standards and frameworks, also called as "best practices", form the basis of any organizational security management effort, and have occupied the center stage of related research (Hsu 2009; Niemimaa and Niemimaa 2017, 2019). We have contributed to these discussions with a new model that has potential to transform how information security is managed in organizations, or to use Vuorinen and Uusitupa's (2022) terms, transform the "ethos" of information security. To the best of our knowledge, this model is the first design attempt to apply the principles of Zero Trust to the organizational aspects making it a novel design artifact (Baskerville et al., 2018; Hevner et al., 2004), which also underlines the design contribution of our research.

Conclusions

This paper shows how a model can be designed for organizations to assess and improve their technical and organizational Zero Trust maturity. Using design science research (Baskerville et al. 2018; Gregor and Hevner 2013), we have developed the EZTMM, a functional holistic maturity model with an accompanying maturity assessment tool. The model was jointly developed with information security experts to ensure its relevance but also high quality. The model has been evaluated through a case study which indicates its practical usability and usefulness. Further, our naturalistic case study evaluation of the artifact indicates that it fulfills the design goals. Our primary contributions are:

- *Theoretical contributions:* The designed model is a novel contribution to IS security management literature by providing a model that is founded on the Zero Trust principles and provides a holistic approach (May & Dhillon, 2010; Soomro et al., 2016).
- *Design contributions:* Our research applies socio-technical perspective to the context of Zero Trust to design a model that covers people, processes, and technology. As such, the model is an extension and exaptation (Gregor & Hevner, 2013) of existing ideas from technology research to address organizational information security problems. Further, the instantiation of socio-technical perspective as maturity model artifact generates new design knowledge.
- *Practical contributions:* Our research provides practitioners with a readily available and usable model that organizations and their information security experts can use to evaluate organizational and technical maturity on Zero Trust. Further, the evaluation can serve as the basis for developing organizational Zero Trust maturity.

This study has limitations. The EZTMM has been evaluated only in one country, and mostly in large organizations, and long-term effectiveness has not been evaluated, as is typical for design science research papers where an artifact is constructed (Maedche et al. 2021). Furthermore, not all the suggested improvements based on the evaluation have been integrated into the EZTMM. These provide possible avenues for further research and development of the EZTMM.

References

Ahmed, M., and Petrova, K. 2020. “A Zero-Trust Federated Identity and Access Management Framework for Cloud and Cloud-Based Computing Environments,” *WISP 2020 Proceedings*.

Almuhammadi, S., and Alsaleh, M. 2017. “Information Security Maturity Model for Nist Cyber Security Framework,” in *Computer Science & Information Technology (CS & IT)*, Academy & Industry Research Collaboration Center (AIRCC), February 25, pp. 51–62.

Backhouse, J., Hsu, C. W., and Silva, L. 2006. “Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard,” *MIS Quarterly* (30), pp. 413–438.

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A. R., and Rossi, M. 2018. “Design Science Research Contributions: Finding a Balance between Artifact and Theory,” *Journal of the Association for Information Systems* (19:5), pp. 358–376.

Becker, J., Knackstedt, R., and Pöppelbuß, J. 2009. “Developing Maturity Models for IT Management,” *Business & Information Systems Engineering* (1:3), pp. 213–222.

Bostrom, R. P., and Heinen, J. S. 1977. “MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes,” *MIS Quarterly* (1:3), Management Information Systems Research Center, University of Minnesota, pp. 17–32.

Braden, R. T. 1989. “Requirements for Internet Hosts - Communication Layers,” Request for Comments No. RFC 1122, Request for Comments, Internet Engineering Task Force, October. (https://doi.org/10.17487/RFC1122).

Buck, C., Olenberger, C., Schweizer, A., Völter, F., and Eymann, T. 2021. “Never Trust, Always Verify: A Multivocal Literature Review on Current Knowledge and Research Gaps of Zero-Trust,” *Computers & Security* (110), p. 102436.

Choobineh, J., Dhillon, G., Grimaila, M. R., and Rees, J. 2007. “Management of Information Security: Challenges and Research Directions,” *Communications of the Association for Information Systems* (20), pp. 958–971.

Chouikh, A., Khechine, H., and Gagnon, M.-P. 2023. “Developing a Maturity Model for Information Security Awareness Using a Polytomous Extension of the Rasch Model,” *Proceedings of the 56th Hawaii International Conference on System Sciences (HICSS)*. (https://hdl.handle.net/10125/103461).

CISA. 2021. “Zero Trust Maturity Model,” CISA. (https://www.cisa.gov/zero-trust-maturity-model).

Coles-Kemp, L. 2009. “Information Security Management: An Entangled Research Challenge,” *Information Security Technical Report* (14:4), Human Factors in Information Security, pp. 181–185.

Cram, W. A., D’Arcy, J., and Proudfoot, J. G. 2019. “Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance,” *MIS Quarterly* (43:2), pp. 525–554. (https://doi.org/10.25300/MISQ/2019/15117).

De Bruin, T., Rosemann, M., Freeze, R., and Kaulkarni, U. 2005. “Understanding the Main Phases of Developing a Maturity Assessment Model,” in *Australasian Conference on Information Systems (ACIS)*, D. Bunker, B. Campbell, and J. Underwood (eds.), CD Rom: Australasian Chapter of the Association for Information Systems, pp. 8–19.

Dlamini, M. T., Eloff, J. H. P., and Eloff, M. M. 2009. “Information Security: The Moving Target,” *Computers & Security* (28:3), pp. 189–198.

Eloff, J. H. P., & Eloff, M. M. (2005). Information security architecture. *Computer Fraud & Security*, *2005*(11), 10–16.

Gottschalk, P., and Solli-Saether, H. 2009. *E-Government Interoperability and Information Resource Integration: Frameworks for Aligned Development: Frameworks for Aligned Development*, Idea Group Inc (IGI).

Gregor, S., and Hevner, A. R. 2013. “Positioning and Presenting Design Science Research for Maximum Impact.,” *MIS Quarterly* (37:2).

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

Hsu, C. W. 2009. “Frame Misalignment: Interpreting the Implementation of Information Systems Security Certification in an Organization,” *European Journal of Information Systems* (18:2), pp. 140–150.

Järveläinen, J., Niemimaa, M., and Zimmer, M. P. 2022. “Designing a Thrifty Approach for SME Business Continuity: Practices for Transparency of the Design Process,” *Journal of the Association for Information Systems* (23:6), pp. 1557–1602.

Kindervag, J., Balaouras, S., Mak, K., and Backborow, J. 2016. “No More Chewy Centers: The Zero Trust Model Of Information Security,” Forrester Research, March 23, pp. 1–18. (https://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf).

Kuechler, B., and Vaishnavi, V. 2008. “On Theory Development in Design Science Research: Anatomy of a Research Project,” *European Journal of Information Systems* (17:5), Palgrave Macmillan Ltd., pp. 489–504.

Lacity, M., and Carmel, E. 2022. “Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet,” *MIS Quarterly Executive* (21:3).

Lain, D., Kostiainen, K., and Čapkun, S. 2022. “Phishing in Organizations: Findings from a Large-Scale and Long-Term Study,” in *2022 IEEE Symposium on Security and Privacy (SP)*, pp. 842–859.

Lee, C. H., Geng, X., and Raghunathan, S. 2016. “Mandatory Standards and Organizational Information Security,” *Information Systems Research* (27:1), pp. 70–86.

Lowry, P. B., Dinev, T., and Willison, R. 2017. “Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda,” *European Journal of Information Systems* (26:6), pp. 546–563.

Maedche, A., Gregor, S., and Parsons, J. 2021. “Mapping Design Contributions in Information Systems Research: The Design Research Activity Framework,” *Communications of the Association for Information Systems* (49:1), Association for Information Systems, p. 12.

May, J., and Dhillon, G. 2010. “A Holistic Approach for Enriching Information Security Analysis and Security Policy Formation,” in *ECIS 2010 Proceedings*.

McKnight, D. H., Cummings, L. L., and Chervany, N. L. 1998. “Initial Trust Formation in New Organizational Relationships,” *Academy of Management Review*, Academy of Management Briarcliff Manor, NY 10510.

Modderkolk, M. G. 2018. “Zero Trust Maturity Matters: Modeling Cyber Security Focus Areas and Maturity Levels in the Zero Trust Principle,” Master Thesis, Master Thesis. (https://studenttheses.uu.nl/handle/20.500.12932/29189).

Mumford, E. 2006. “The Story of Socio-Technical Design: Reflections on Its Successes, Failures and Potential,” *Information Systems Journal* (16:4), pp. 317–342.

Myers, M. D., and Newman, M. 2007. “The Qualitative Interview in IS Research: Examining the Craft,” *Information and Organization* (17:1), pp. 2–26.

Niemimaa, E., and Niemimaa, M. 2017. “Information Systems Security Policy Implementation in Practice: From Best Practices to Situated Practices,” *European Journal of Information Systems* (26:1), Springer, pp. 1–20.

Niemimaa, M., and Niemimaa, E. 2019. “Abductive Innovations in Information Security Policy Development: An Ethnographic Study,” *European Journal of Information Systems* (28:5), Taylor and Francis Ltd., pp. 566–589.

Office of Cybersecurity, Energy Security, and Emergency Response. 2021. “Cybersecurity Capability Maturity Model (C2M2), Version 2.0,” Office of Cybersecurity, Energy Security, and Emergency Response, July.

Paulk, M. C., Curtis, B., Chrissis, M. B., and Weber, C. V. 1993. “Capability Maturity Model, Version 1.1,” *IEEE Software* (10:4), pp. 18–27.

Pöppelbuß, J., Niehaves, B., Simons, A., and Becker, J. 2011. “Maturity Models in Information Systems Research: Literature Search and Analysis,” *Communications of the Association for Information Systems* (29:1).

Pöppelbuß, J., and Röglinger, M. 2011. “WHAT MAKES A USEFUL MATURITY MODEL? A FRAMEWORK OF GENERAL DESIGN PRINCIPLES FOR MATURITY MODELS AND ITS DEMONSTRATION IN BUSINESS PROCESS MANAGEMENT,” *ECIS 2011 Proceedings*.

SABSA. 2019. “The Attributer’s Blog - Zero Trusted,” *The SABSA Institute*, , February 27. (https://sabsa.org/the-attributers-blog-zero-trusted/, accessed May 3, 2023).

Saleh, M. 2011. “Information Security Maturity Model,” *International Journal of Computer Science and Security (IJCSS)* (5), p. 21.

Sarker, S., Chatterjee, S., Xiao, X., and Elbanna, A. 2019. “The Sociotechnical Axis of Cohesion for the IS Discipline: Its Historical Legacy and Its Continued Relevance,” *MIS Quarterly* (43:3), pp. 695–720.

Schlette, D., Vielberth, M., and Pernul, G. 2021. “CTI-SOC2M2 – The Quest for Mature, Intelligence-Driven Security Operations and Incident Response Capabilities,” *Computers & Security* (111), p. 102482.

Silic, M., and Back, A. 2014. “Information Security: Critical Review and Future Directions for Research,” *Information Management & Computer Security* (22:3), Emerald Group Publishing Limited, pp. 279–308.

Siponen, M., and Willison, R. 2009. “Information Security Management Standards: Problems and Solutions,” *Information & Management* (46:5), pp. 267–270.

Slovic, P. 1993. “Perceived Risk, Trust, and Democracy,” *Risk Analysis* (13:6), pp. 675–682.

Soliman, W., & Ojalainen, A. (2023). Conflict Resolution in an ISO/IEC 27001 Standard Implementation: A Contradiction Management Perspective. *56th Hawaii International Conference on System Sciences*, 4839–4848.

Soomro, Z. A., Shah, M. H., and Ahmed, J. 2016. “Information Security Management Needs More Holistic Approach: A Literature Review,” *International Journal of Information Management* (36:2), pp. 215–225.

Thuan, N. H., Drechsler, A., and Antunes, P. 2019. “Construction of Design Science Research Questions,” *Communications of the Association for Information Systems* (44:1), pp. 332–363.

Venable, J., Pries-Heje, J., and Baskerville, R. 2016. “FEDS: A Framework for Evaluation in Design Science Research,” *European Journal of Information Systems* (25:1), pp. 77–89.

Vom Brocke, J., Winter, R., Hevner, A. R., and Maedche, A. 2020. “Special Issue Editorial – Accumulation and Evolution of Design Knowledge in Design Science Research: A Journey through Time and Space,” *Journal of the Association for Information Systems* (21:3), pp. 520–544.

Vuorinen, J., and Uusitupa, V. 2022. “Zero Trust Model and the Shift in the Ethos of Cybersecurity – Towards the Deleuzian Society of Control,” in *Ethicomp 2022 Proceedings*, J. Koskinen, K. Kimppa, O. Heimo, J. Naskali, S. Westerstrand, and M. Rantanen (eds.), , September 6.

Whitman, M. E. 2003. “Enemy at the Gate: Threats to Information Security,” *Communications of the ACM* (46:8), pp. 91–95.