On the Design and Engineering of a Zero Trust Security Artefact

Yuri Bobbert[1,2(✉)] and Jeroen Scheerder[2]

[1] University of Antwerp, Antwerp, Belgium
yuri.bobbert@on2it.net
[2] ON2IT, Zaltbommel, Netherlands
jeroen.scheerder@on2it.net

Abstract. Adequately informing the board of directors about operational security effectiveness is cumbersome. The concept of Zero Trust (ZT) approaches information and cybersecurity from the perspective of the asset, or sets of assets, to be protected, and from the value that it represents. Zero Trust has been around for quite some time. This paper continues on the authors previous research work on the examination of Zero Trust approaches, what is lacking in terms of operationalisation and which elements need to be addressed in future implementations and why and how this requires empirical validation. In the first part of the paper, we summarise the limitations in the state of the art approaches and how these are addressed in the Zero Trust Framework developed by ON2IT 'Zero Trust Innovators'. Then we describe the design and engineering of a Zero Trust artefact (dashboard) that addresses the problems at hand, according to Design Science Research (DSR). The last part of this paper outlines the setup of an empirical validation trough practitioner-oriented research, in order to gain a better implementation of Zero Trust strategies. And how this validation was conducted in 2020 with 73 security practitioners. The final result is a proposed framework and associated technology which, via Zero Trust principles, addresses multiple layers of the organization to grasp and align cybersecurity risks and understand the readiness and fitness of the organization and its measures to counter cybersecurity risks.

Keywords: Zero Trust security · Architecture · Cybersecurity · Digital Security · Managed Security Services (MSS) · Security Operation Centre (SOC) · Security strategy · Design Science Research (DSR) · Group Support System (GSS) · Platform technology · Security Orchestration · Automation and Response (SOAR)

1 Introduction

These days it's impossible to imagine business without technology. Most industries are becoming "smarter" and more tech-driven — ranging from small individual tech initiatives to complete business models with intertwined supply chains and "Platform" based business models [1]. New ways of working such as Agile and DevOps are introduced and thereby new risks arise [2, 3]. Not only technology risks, but also risks that are

K. Arai (Ed.): FICC 2021, AISC 1363, pp. 830–848, 2021.
https://doi.org/10.1007/978-3-030-73100-7_58

caused by teams working together at high pace and autonomy [4, 5]. Where decisions on risk acceptances or security measures most of the time take place in the team itself rather than looking at the bigger picture of accumulated risks [6]. According to CRO-Forum[1] this is an increasing "silent risk" [3]. This autonomous way of working in agile teams – in most case in a distributed manner- is needed to enable speed, quality and craftmanship and there is a quicker time to market [7]. For policymakers and business leaders technology is no longer a domain that is shrouded in mystery; rather it's an essential business discipline that is here to stay, and it's taught at business schools all over the world. It's also a professional discipline that has won the attention of analysts and supervisory boards. However, at the same time, nefarious nation -state activity and organized crime have arrived on the scene in a big way. Through hacks and denial-of-service attacks, all sorts of malicious actors are infiltrating our 'digital' society. They can easily take advantage of systems that are sloppily designed, built and configured and they frequently use advanced "socially engineering" techniques to trick their way into organizations. Platform oriented businesses are typically built on api-based-ecosystems of data, assets, applications and services (DAAS). These hybrid technology landscapes, most of the time built-in software defined networks in clouds [8], lack real-time visibility and control when it comes to their operations [9, 10]. This makes it hard for boards to take ownership and accountability of cyber risks [11]. In practice, we have seen the application of security and privacy frameworks falter because they tend to become a goal on their own rather than a supporting frame of reference to start dialogues with key stakeholders [12]. Kluge et al. [13] for example also noted that the use of frameworks as a goal on its own does not support the intrinsic willingness and commitment to improve. This is especially the case for mid-market organizations that lack dedicated security staff, capabilities and/or sufficient budgets [14]. Puhakainen and Siponen [15] noted that information security approaches are lacking not only theoretically grounded methods, but also empirical evidence of their effectiveness. Many other researchers [16–18] have also pointed out the necessity of empirical research into practical interventions and preconditions in order to support organizations improve the effectiveness of their security. These theoretical voids, as well as the practical observation of failing compliant-oriented approaches, widen the knowledge gap [19]. This "knowing-doing gap" [20] is also perceived in the current Zero Trust approaches, which predominantly aim at the technology or by the technology industry. In our previous paper published in June, titled "Zero Trust Validation: From Practical Approaches to Theory" [21] we have described the several streams of Zero Trust, such as security vendors aiming to deliver point solutions for Zero Trust security and why ON2IT developed a Framework that addresses the problems we describe in the next section.

2 Problem

Although the term "Zero Trust" can be perceived that individuals, i.e. human beings cannot be trusted, Zero Trust actually implies humans can be trusted, but always need

[1] Chief Risk Officer Forum; The CRO Forum's Emerging Risk Initiative continually scans the horizon to identify and communicate emerging risks.

to be verified *before* access and authorization is granted. Jagasia quotes; *"perimeter-based security primarily follows "trust and verify," which is fundamentally different from ZTA's paradigm shift of "verify, and then trust."* Kindervag formulates it more strongly: we have to get rid of the concept of trust: *"The point of Zero Trust is not to make networks, clouds, or endpoints more trusted; it's to eliminate the concept of trust from digital systems altogether.* Kindervag proceeds with; *"We've injected this concept of trust into digital systems, but it should have never been there, because trust represents a vulnerability for digital systems"* [22].

Since its Zero Trust inception in 2010, research and consulting firm Forrester puts forward the thought leadership of Kindervag [22] in their approaches, focusing mainly on managerial level but lacking operational detailing that DevOps teams and engineers can get proper guidance from. Most of the security measures are derived from the control objectives in control frameworks and are not directly aligned with security measures prescribed by tech vendors. Consequently, linking the strategic objectives to operational security measures is complex and is rarely implemented [18]. The problem with an approach that lacks alignment with strategic goals lies in the limitations of mainly IT-focused security and security experts. Bobbert refers to operating in silo's without any reflection outside the silo [23]. The security experts operate in silos with limited view on the world and the business drivers and business context [19]. This is important, as information security is subject to many different interpretations, meanings and viewpoints [24], especially since major breaches can have serious impact on the continuity of the firm as well as their individual board members [25]. Bobbert states in his research into improving Business information security that it needs to be a collaborative effort between Technology, Business (Asset Owners) and risk management to establish and maintain a proper and -near- real-time Cyberrisk and security administration. From strategic level towards the operations and vice versa. To effectively link the strategic level of the organization to the operational level in the organization, we need to have a proper level of awareness and understanding on *how* to do this. We explore this challenge based on

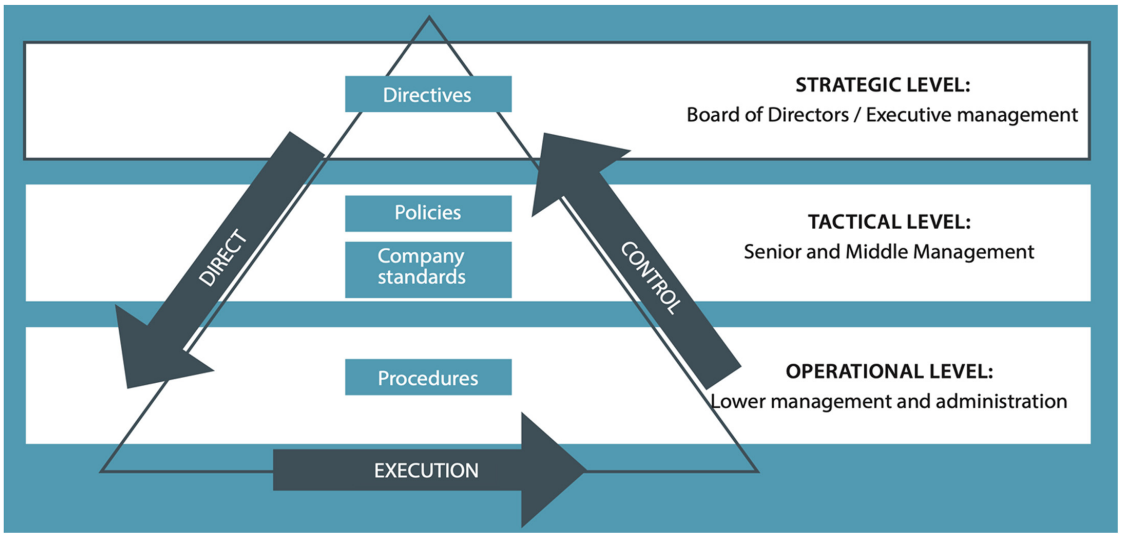

Fig. 1. The IS Governance Direct Control Cycle taken from Von Solms and Von Solms [26] and applied in ISACA's COBIT5 Framework for Enterprise Governance of IT.

earlier research in this domain, distinguishing per organizational level the processes and data.

2.1 Business Information Security Processes and Data

The Information Security Governance (ISG) layers to bridge the so called knowing-doing [20] gap and to gain the integral view the Von Solms brothers developed the Direct Control Cycle [26] (Fig. 1). The authors distinguish three levels of the organisation: Governance, Management and Operational level.

We elaborate on each level, including some examples. The directive-setting objectives stem from the strategic level. Risk appetite and accompanying policies are communicated to senior management in the form of requirements. Senior management is then mandated to put these policies into standards (e.g. technical, human and process requirements). These standards are applied in terms of all kinds of risks (e.g. through maintenance of risk logs) and security (e.g. security action plans, advisories) processes and controls (e.g. general IT controls). Processes and controls depend on underlying processes such as operational services processes like: change management, configuration management, incident management and problem management. All with clear requirements. Due to changes in legislation, technological trends (Cloud, IoT, OT, Big Data) and changing business environments, the subsequent security requirements also change. In many organizations, these requirement-setting documents reside on personal laptops, fileshares (e.g. sharepoint), desktops in spreadsheets [27]. This Excel spreadsheet based way of working generates an administrative burden to maintain and becomes a risk on its own since there is no single, authoritative place of truth [2].

2.2 Problem Statement

This problem becomes bigger with the growth of all sorts of smart devices and data sitting all over the place. Regulated companies perform better in this respect, since managing information risk and security is part of their license to operate and losing that poses a business continuity risk. Continuous measurement and reporting on the performance of risk and security processes is needed in order for senior business leaders to take ownership of assets and risks, due to rotation of personnel, the introduction of new tech-services without IT involvement, formal procurement processes (vendor vetting, etc.), mergers and acquisitions, rough and orphan assets become the new standard rather than an exception. Accurate administration of critical assets, the value they represent, CIA ratings etc. is not in place nor centrally administered. This wood of security tooling causes decision latency[2], during a hack, due to inefficient security operations that has limited interaction. The tools are owned, consumed, managed and measured by multiple stakeholders like auditors, managers, security staff, IT, business users. This brings us to the main problem statement, which is:

[2] The Standish Group: Decision latency theory states: "The value of the interval is greater than the quality of the decision." Therefore, to improve performance, organizations need to consider ways to speed-up their decisions.

"Current emphasis of Zero Trust lies on architecture principles that are understood only by insiders. The current approaches and documents lack alignment with risk management, existing frameworks and associated processes. Board and business involvement are not addressed and ownership of data, risks, security controls and processes is limited. And the main focus is on the change and not on the run and its value contributors".

2.3 Research Questions

Pondering the issues mentioned above there is a need to establish a more collaborative way of working among stakeholders when addressing the dynamics of the environment and the organization, gain a more qualitative and integral view based on facts related to tactical and operational data, to secure an increase in awareness at board level, to cultivate a certain level of reflection and self-learning and improvement to use recognised best-practice frameworks produced and maintained by existing communities. Therefore, the aim of this research is to answer the following main research question "*How can we establish a method which utilizes best practices and collaboration for improving Zero Trust security implementations?*".

In order to answer this main research question, we follow Wieringa [28] to distinguish Knowledge Questions (KQ) and Design Questions (DQ). Knowledge questions provide us with insights and learnings that together with Design Questions contribute in the construction of the design artefact (later referred to as Portal) since the artefact will be integrated in the exiting Managed Security Service Portal (MSSP) of ON2IT. This means that during the Design and development stages separate –requirement- design questions are formulated with the objective to design artefact requirements. The Design Science Research Framework of Johannesson and Perjons [29] is adopted and visualized in Fig. 2. This approach follows earlier design and engineering efforts at the University of Antwerp and Radboud University [9, 2].

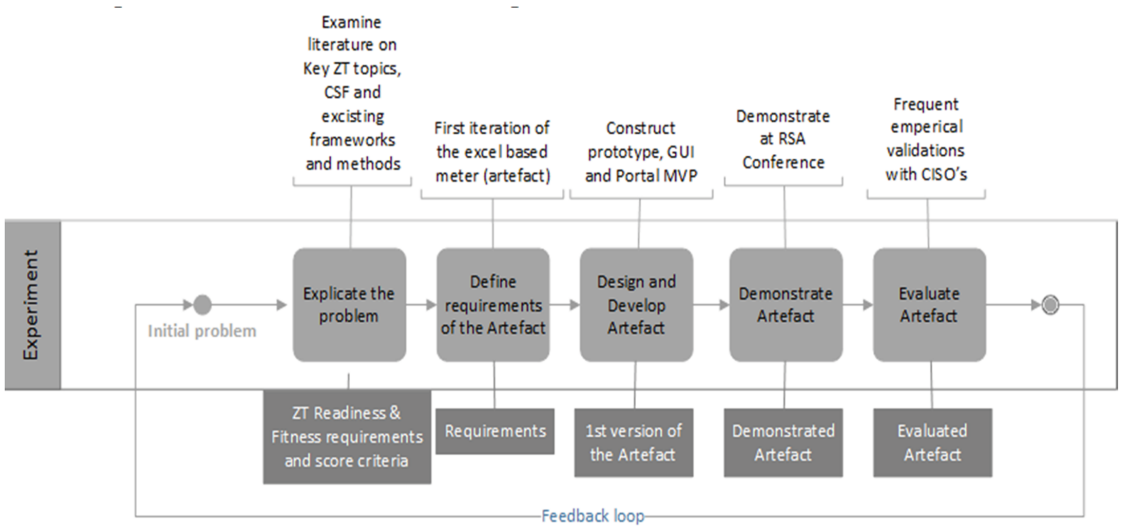

Fig. 2. Conceptual model for the Zero Trust Framework and artefact based on Design Science Research (Taken from Perjon and Johannesson) as proposed in the authors earlier research work [21]

In our previous publication we have formulated the following research questions:

1. What are Critical Success Factors for drafting and implementing a ZTA?
2. What is an easy to consume capability maturity -readiness- model and its associated portal technology that enables the adoption of ZTA and guides boards and management teams and facilitates collaboration and ownership?
3. How does the future empirical validation of the framework and the associated portal look like and how does it provide feedback to relevant stakeholders?

3 Research and Development Methodology

Design Science Research (DSR) has attracted increasing interest in the Information System research domain. March and Mith initiated important DSR work with their early paper on a two-dimensional framework for research on information technology [30]. The objective of DSR research is to establish artefacts that solve real-life problems. The collective set of requirements within the DSR artefact should contribute in this goal. Frequent validation involving stakeholders, such as users, engineers and customers to confirm that the artefact requirements actually help solve the problem at hand is necessary [31]. Wieringa [31] refers to using the regulative cycle to determine the right set of artefact requirements and to validate if it contributes to solving the problem.

Hevner et al. [32] produced a broad framework which is used worldwide to perform and publish DSR work. This framework is visualized in see Fig. 3 contrasts two research paradigms in information system research: *behavior sciences* and *design sciences*. Both domains are relevant for Information Security because the first is concerned with soft aspects such as the knowledge, attitudes and capabilities required to study and solve problems. The second is concerned with establishing and validating artefacts. To put it more precisely, Johannesson and Perjons distinguish between the design, development, presentation and evaluation of an artefact [29]. Wieringa distinguished many methods for

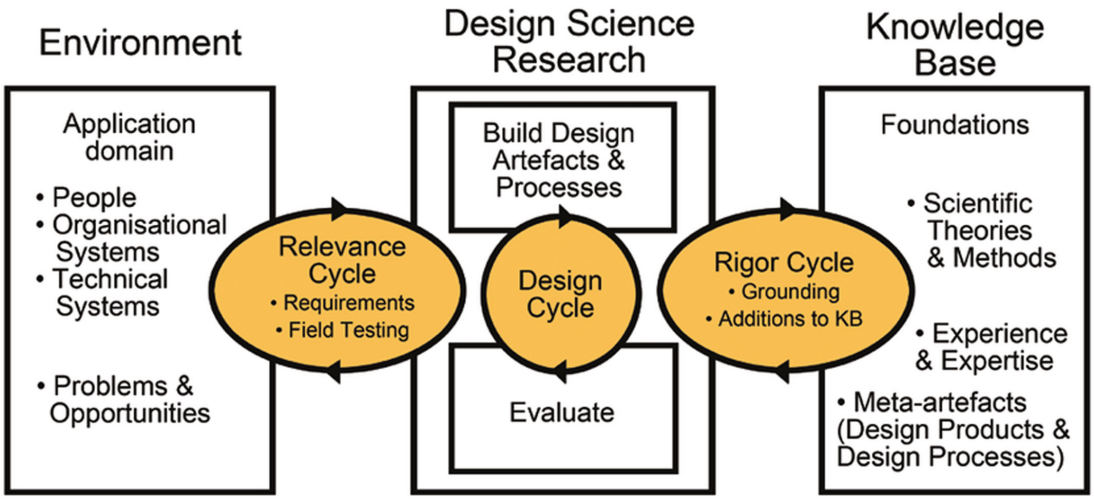

Fig. 3. Hevner's Design Science Research Framework [32].

examining numerous types of problems, e.g. design problems and knowledge problems [33]. In this Zero Trust project we used Hevner's work as a frame of reference for the entire DSR project and potential later validation by practitioners and we use Wieringa's approach to address the challenges and technical requirements we encounter during the current and future journey of portal development.

Design Science Research in a Business Context
Like any other longitudinal research new insights emerged from the problems we encountered in real life environments during the performance of our research project. The complete project, specifically the design of the artefact, is done in a practical business setting. We applied the research strategy displayed in Fig. 4, departing conducting literature research on main ZT topics and shortcomings. This was largely published in our research paper: "Zero Trust Validation: From Practical Approaches to Theory". That research paper mainly focusses on phase 1 and 2. This research paper manly focusses on 3, 4 and 5.

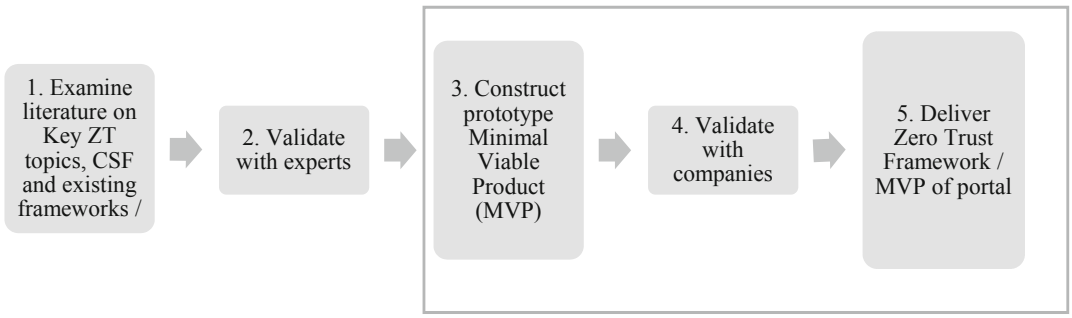

Fig. 4. Scope of the research project and strategy to design and build the Zero Trust Framework and portal technology (artefact) based on DSR.

4 Results of the Research

Based upon the above-mentioned insights from the literature and experiences we have detailed the Critical Success Factors in our previous publication, being; *Engage and collaborate with relevant stakeholders* on the value of Zero Trust for the business. *Alignment with existing control framework* and their scaling, metrics and taxonomy so it enables collaboration. *Complete and accurate administration* of critical assets (Data, Assets, Applications, Services: DAAS), CIA rating and their security requirements in a central repository (one source of truth). Establish a *Clear technology roadmap* with Zero Trust based measures that have a clear definition of done (DoD) and timelines for implementation.

As a result of the previous publication, Bobbert & Scheerder proposed a longitudinal research methodology to do empirical research with Chief Information Security Officer (CISO's) and Data Protection Officer (DPO's) on validating this Framework collectively due to group collaboration in small groups [34]. This research paper continues on that research proposition of longitudinal research. Table 1 shows the ON2IT Zero Trust Framework and the Three Organizational Levels.

Table 1. The ON2IT Zero Trust Framework and the Three Organizational Levels According to the Direct Monitor and Control Cycle

Strategic/Governance	*Know your environment and capabilities*	Determine to what extend context analysis, leadership capabilities, roles, and accountabilities are in place to execute a Zero Trust strategy
Managerial	*Know your risks*	Determine to what extend structures, processes, and relational mechanisms (reporting, roles, tone at the top, and accountabilities) are in place to execute the strategic zero trust objectives. E.g. Capabilities for logical segmenting[a]
Operations	*Know your technology*	Determine to what extent current or future technology is able to utilize zero trust measures. (Fitness)

[a]Segment being "A logical part of the environment which consist of collaborating data, assets, applications and services that represent a certain value, business dependency and exposed to certain risks".

5 Alignment of the ON2IT Zero Trust Framework

To answer research question two;

> *"What is an easy to consume capability maturity -readiness- model and its associated portal technology that enables the adoption of ZTA and guides boards and management teams and facilitates collaboration and ownership?"*

Rendering to the aforementioned shortcomings, obtained from the literature, the improved framework has the objective to function as guidance for senior managers and boards, before they start a Zero Trust strategy. In this section we recall the improvements put forward in our previous paper, in the next section we demonstrate how the Framework and Portal artefact addresses just that:

- A common language is used by making use of existing control Framework. This makes it an easy to consume model.
- The Framework enforces strict sign off for asset owners and board members on preconditions that are required before you can implement Zero Trust.
- Segmenting the environment based on data flows; Each Data, Application, Asset or Service (DAAS) element in a segment requires ownership and annotation of the level of Confidentiality, Integrity and Availability (CIA) in a central repository to ensure sufficient asset qualification so security measures can be assigned to these assets.
- By assessing the readiness and technological fitness to utilize Zero Trust there is transparency in the level of a successful ZT implementation, the "progress monitor" in the framework monitors the progress.

6 From Zero Trust Strategy to Operations

In the Zero Trust architecture, measures are implemented to limit the attack surface, and to provide visibility and, hence, swift and to-the-point incident response.
How we allocate measures to segments is described below. First, by identifying traffic flows relevant to a (closely coupled) application. In physical networks, the notion of segmentation takes a step further; the term 'microsegments' has been coined. By intention, such segments contain a (functional) application or a set of closely associated applications. By this additional segmentation, a 'microperimeter' is formed that can be leverage to exert control over, and visibility into, traffic to/from the contained (functional) application. A policy governs the traffic flows, inspects those flows and thereby the Zero Trust architecture not just prescribes defence in depth by isolation but also by inspection, response and reporting. We will elaborate this in more specific detail;

- Policy regulating traffic to and from a Zero Trust segment

  o s *specific* and *narrow*, satisfying the 'least privilege access' principle: it allows what's functionally necessary, and *nothing more*;
  o is, whenever possible, related to (functional) *user groups*
  o enforces that traffic flows contain *only* the network applications that are defined for that specific segment;
  o enforces content inspection to enable threat detection and mitigation on;
  o visibility is ensured;

- Logs are, whenever possible, related to *individual users*;
- Presence and conformance of policy is operationally safeguarded;
- Policy is *orchestrated*, if applicable, across multiple components in complex network paths;
- Operational state and run-time characteristics (availability, capacity instrumentation) are structurally monitored.
  The very same concepts applied above to physical networks are used, unchanged, in virtual-, container-, cloud- or other software defined networks. In all cases, a way is found to create a logical point of 'visibility and control' that enables insertion and safeguarding of the appropriate measures.
  Extending the Zero Trust architecture to endpoints is a step that is conceivable as well, considering the endpoint itself as a complex collective of potentially unwanted (malicious) processes to be safeguarded. At endpoint level, an agent can be introduced to detect and mitigate malicious processes. When doing this, fine-grained endpoint behaviour extends the visibility beyond the network layer, and 'large data' analysis of (user) behaviour becomes viable, further deepening both visibility and defence in depth. Extracting the telemetry data -near- real time from these technological measures is needed to feed this data back to tactical and strategical levels and promptly respond and telecommand back[3]. This relates to the increasing question; "*how to inform the CEO in minutes after a breach?*

[3] Telemetry is the collection of measurements or other data at remote or inaccessible points and their automatic transmission to receiving equipment for monitoring. The word is derived from

7 Deliverables

- Due to practical experiences we see that an important factor for Zero Trust success is to start with assessing the organizations readiness and technological fitness to adopt and execute Zero Trust. Therefore the "Framework" should follow a certain sequence of application, as displayed in Fig. 5, initially consist of:
- A Readiness assessment to determine how ready and fit you are as a company on the strategic level and managerial level.
- An assessment to determine your technological fitness compared to objectives. This fitness level represents to what extent an organization is technically capable of utilizing the required Zero Trust measures and understand their limitations. Starting with five segments to aid the learning curve and understand the earlier mentioned Knowing Doing Gap.
- A process of labelling these five segments with meta-data such as CIA ratings, Relevance scores, regulatory-compliance tags. This is desired to determine the technical policies and guidelines that should be applied to the segments. Table 2 displays the Relevance score and associated DAAS label. Determining the relevance score can be done by making use of existing CIA rating methods. Where CIA normally rates the asset, will the Relevance score rate the entire segment with potentially multiple assets.

Table 2. Overview of the Relevance Score and the DAAS Labels in the Artefact (Portal)

Relevance score	Detailing	DAAS Label
0–25 (CI11)	No personal data, no sensitive data, limited number and amount of financial data. No possible legal, contractual or regulatory impact. Minor local reputational damage possible. Medium financial impact	
25–50 (CI22)	Limited amount of personal data (<4 different data types) and a limited amount of data subjects, no sensitive data, limited number and amount of financial data. No possible legal, contractual or regulatory impact. Minor local reputational damage possible. Medium financial impact	Subject to audit, Core processing 3rd party access to data Personal data (PII)
50–75 (CI33)	Personal data or financial data available, Legal, contractual, or regulatory impact possible. Reputational damage can be locally impacted. High financial impact. Industrial Control Systems with High availability. (with business case and all applies with potential waiver process)	Personal data (PII) Core processing 3rd party access to data Confidential data
75–100(CI44)	Special personal data or sensitive financial data available. Serious Legal, contractual, or regulatory impact (serious fines, suspension or loss of license) possible. Risk of sustained (inter)national reputational damage. Industrial Control Systems with High availability requirements. Very high financial impact. (At any cost)	Special personal data, Industrial Control Systems Personal data (PII) Core processing 3rd party access to data Confidential data

Greek the roots tele, "remote", and metron, "measure". Systems that need external instructions and data to operate require the counterpart of telemetry, telecommand. Source.

- A Progress Monitor to report to boards and regulators on a periodical basis and thereby involve them in the required decision making and avoid decision latency. An additional portal functionality built into the ON2IT Managed Security Services Platform Portal (also referred to as an *artefact*) that captures; a. the readiness assessment results on the three levels of strategy, management and operations, b. the Zero Trust segments with meta-data and c. the fitness score of the segments extracted from the operational technology by ingesting logs of technology such as segmentation gateways a.k.a. firewalls, end points and other security measures.

The operationalization of the ON2IT Zero Trust Framework is done in the portal. We detail per Framework component "how" this is operationalized and evidenced in this paper by making use of portal screenshots.

Figure 6 displays the Zero Trust overall score, the progress of ZT implementation and the Readiness maturity level on strategic and tactical level.

Figure 7 shows the screenshot of the Readiness assessment results on Strategy (including example of "Ownership and sign off" criteria and score).

Figure 8 shows the screenshot of the Fitness assessment results for segment ATMS, including status per measure and in the upper right corner the ZT Heatmap. This heatmap displays the relevance score compared to the security gap (amount of security measures implemented in the specific segments). Segments with a high relevance score but large security gap are calculated in "red zone" of this heatmap. This enables boards and senior managers to have direct insights into weak spots and where to take action.

Figure 9 shows the screenshot of the Fitness assessment results for segment ATMs, including status per measure (e.g. Encryption) and in the lower left corner, the tags for the application of various Standards and frameworks.

Figure 10 shows the screenshot of the operational status of segment "Insurance" with ownership, relevance score and cyber events; exfiltrations, investigations, intrusions, threats and advisories in October 2019.

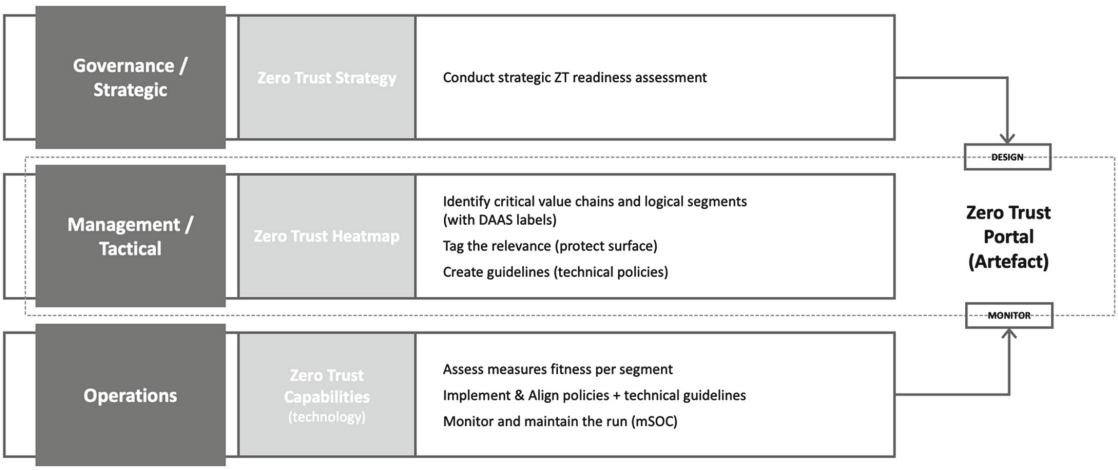

Fig. 5. The ON2IT Zero Trust Framework Approach; from Strategy to Operations

Fig. 6. Screenshot of the Zero Trust Portal (artefact)

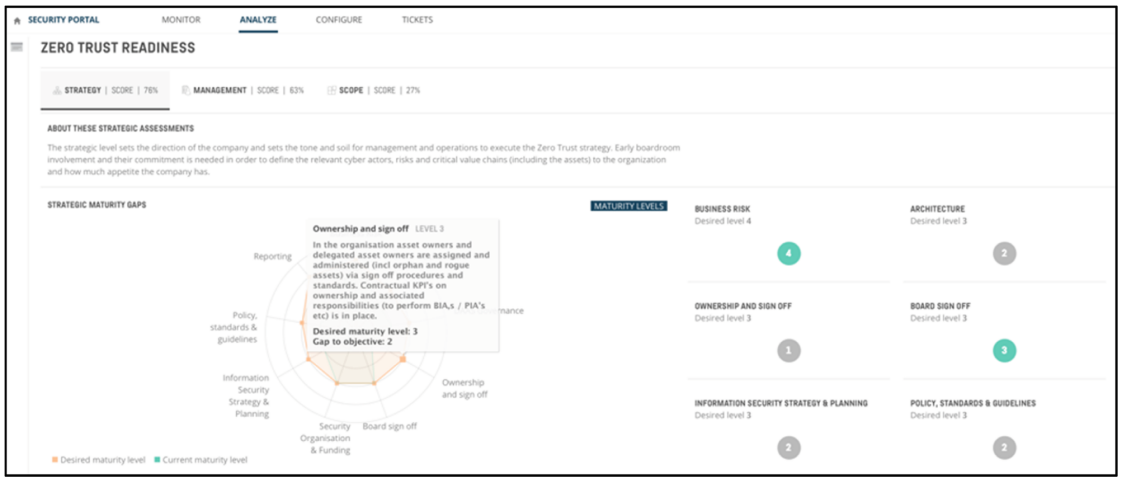

Fig. 7. Screenshot of the Readiness Assessment Results on Strategy (Including Example of "Ownership and Sign Off" Criteria and Score)

8 Preliminarily Results of GSS Validation Sessions

To execute this empirical validation with practitioners, sessions are held and facilitated via Group Support System [9]. The opportunity for larger scale longitudinal research lies specifically in gaining knowledge at the organizational level and using that data, collected with GSS system technologies, to establish a collective knowledge base. This larger set of data can then form a frame of reference for a certain industry, country or community and thus contribute to other sectors, countries or communities. The application of GSS for such large-scale longitudinal research has been identified by De Vreede.

Fig. 8. Screenshot of the Fitness Assessment Results for Segment ATMS (**ATM is** an abbreviation for automated teller machine. The ATM segment is part of the Moore private bank organization used in this demonstration of the artefact), Including Status Per Measure and in the Upper Right Corner the ZT Heatmap

Fig. 9. Screenshot of the Fitness Assessment Results for Segment ATMs, Including Status Per measure (e.g. Encryption). In the Lower Left Corner, the Tags for the Application of Various Standards and Frameworks.

A Group Support System (GSS) method was applied over a period of January 2020 to December 2020 to gain a deeper understanding of the topic, validate the questionnaire questions on clearness and completeness and gather additional viewpoints on Zero Trust. The multiple GSS sessions enabled peer-reflection, which generates new knowledge on the Zero Trust topics. Each group of practitioners developed new insights that were taken into consideration by the next group. This “double-loop learning” [35] provides additional scrutiny to the latter and thereby contributes to the overall quality of the ON2IT Zero Trust Framework. The sessions were executed by a professional GSS moderator, which, according to Hengst, is key [36]. All steps, scores and arguments are recorded in the GSS software to assure objectivity, transparency, controllability and repeatability. A predefined agenda, clear introduction and the readiness questionnaire were shared prior to the meetings so the participants can individually prepare the GSS session.

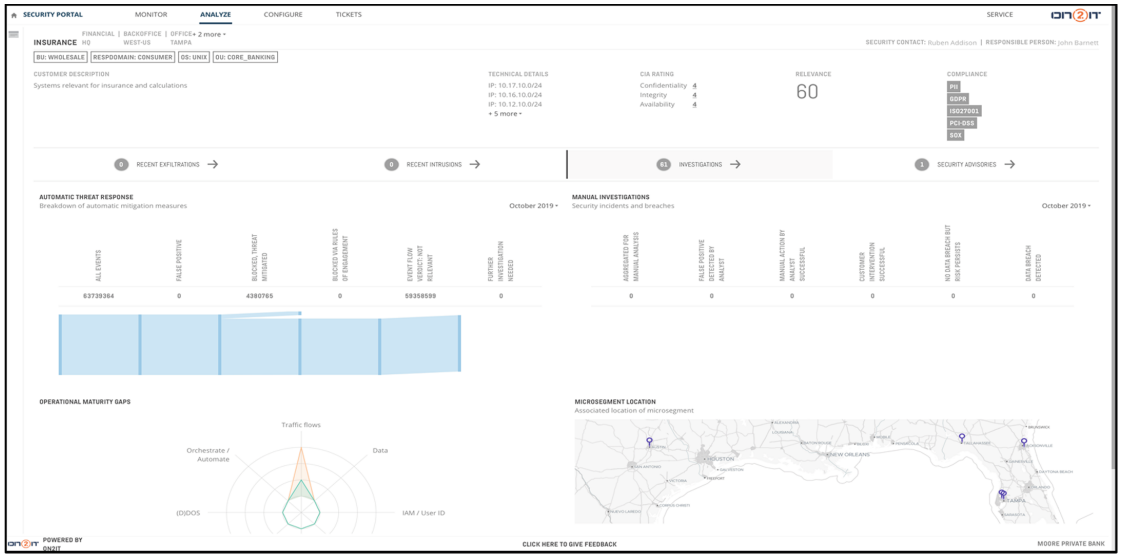

Fig. 10. Screenshot of the Operational Status of Segment "Insurance" with Ownership, Relevance Score and Cyber Events; Exfiltrations, Investigations, Intrusions, Threats and Advisories in October 2019

Process of the GSS Meetups with CISO's and Security Professionals

As proposed in earlier research [21] GSS was used to validate the framework and the associated topics relevant for determining the Readiness maturity level. These questions can function as a questionnaire to diagnose organisations and identify gaps. During 2020 73 participants in 10 sessions validated the framework questions on:

- Completeness, do you have something to complement to the current question set?
- Clearness, is the question easy to understand and without ambiguity?
- Validity, does the set of questions represent topics related to Zero Trust and present in contemporary environments?
- Priority, which one do you think has higher validity over the other and can be prioritised as a core pre-requisite?

Before each session participants were instructed via a clear instruction that included; a video, letter with guidance (including the questionnaire) and once confirmed a phone call to explain:

- Agenda of the session
- Objective of the session
- Expectations of the participants
- Explanation of the process and timelines and required preparation
- The end results

One week prior to each session participants were called to confirm their participation and if preparations were made. Each session was moderated by a professor of Antwerp Management School and professional GSS facilitator. Each of the GSS reports detail:

- The name of the participants;
- Introduction of the session objectives;
- The score of the relevance of the topics and questions, ranking from 1 to 10. 1 being not relevant and 10 being very relevant;
- Comments to the scores per strategic, tactical and operational level;
- Answers to additional questions;
- End evaluation of the session, to verify if objectives are met.

The results of the 10 GSS sessions held among 73 participants with GSS are detailed in the Table 3.

Table 3. Overview of the total amount of GSS participants at strategic level

Validation Session dates in 2020	#Participants
Feb	5
March	7
April	6
May	9
July	4
August	4
September	5
October	6
October	9
Nov	8
Total GSS participants	**73**

Improvements were made to the Framework based upon the empirical validations via GSS. The ON2IT Zero Trust Framework has the objective to act as a guide for boards and managers prior to starting a Zero Trust strategy and during the implementation. Below, we list the major findings for improving the Framework.

- A common language is needed by making use of existing control framework as of level > 3, for example, ISF, NIST Cybersecurity Framework, NIST privacy Framework, PCI DSS or ISO27000 controls. CMMI based maturity levels on a 1 to 5 scale are applied, based on audit terminology (such as Test of Design (ToD), Test of Implementation (ToI) and Test of Effectiveness (ToE)) that NOREA is using.
- Most pf the GSS panel participants acknowledge that Zero Trust can help to inform the CEO quicker, more granular. But Zero Trust can also be viewed as something negative

due to the naming "Zero Trust" that can have a negative perception or aftertaste by boards.
- Following category 1 (Know your environment and capabilities) you identify whether Business, Privacy and IT alignment takes place, threats and trends are identified that influence the enterprise risk management (ERM) and assign appropriate ownership at board and managerial level (according to the COBIT EDM model). On a managerial/tactical level, NIST can be used and on an operational level ISO can be used.

  - COSO / COBIT – Strategic (Enterprise-Level Approach to Risk Management)
  - ISO – Operational (Initiative / Program-Level Approach to Risk Management)
  - NIST – Tactical (Asset / Project-Level Approach to Risk Management)

- A future research project was defined based upon the feedback of the GSS to map all Zero Trust Measures to the SCF framework, that captures all frameworks for Digital Security.
- Each DAAS element requires ownership and CIA annotation in a repository (e.g. CMDB) to ensure adequate asset qualification and even quantification so security measures can be assigned to these assets. A Relevance Score on scale 0–100 combines the standard Business Impact Assessments (BIA) and Privacy Impact Assessment methods (PIA). The presence of personal data, its importance for the Business-critical processes and the type of personal data are all factors that affects the Relevance score, and therefore the type of Security measures to be applies. 0 being a segment with low exposure and 100 with high exposure.
- The Framework encourages strict sign off for board members on preconditions that are required before you can implement Zero Trust. Organizations that use the COBIT5 or COBIT2019 processes and design principles can plot these to the EDM layers of Governance, Management and Operations. This brings the required common language on technical and organizational security measures.
- By assessing the readiness of the organization in terms of processes and structures as well as the technological fitness to utilize Zero Trust transparency is given into the current and desired states. Some participants raised the concerns that in large environments, this segmenting and putting measures in place might take years. Monitoring the progress is vital not to lose attention and urgency.

9 Future Research

To answer research question three: "*How does the future empirical validation of the framework and the associated portal look like and how does it provide feedback to relevant stakeholders?"* can be answered in the following ways:

Assessing an organizations' posture with respect to Zero Trust viability requires evaluating these three levels, *and this ON2IT framework*. We propose four research areas:

1. Validation of the Zero Trust Readiness framework (pre- and post-implementation progress monitor).

2. Assessing the presence and relevance of strategic capability attributes (strategic level).
3. Assessing the presence and relevance of executive capability attributes (managerial level).
4. Assessing the presence and relevance of adequate technical capabilities (operational level).

These assessments determine the relevance, coverage, depth and actionability of the controls/objectives (at their respective level) needed to successfully implement and maintain Zero Trust security strategies.

10 Conclusions

For answering our Research Question; *How can we establish a method which utilizes best practices and collaboration for improving Zero Trust security implementations?"* the ON2IT Zero Trust Framework explicitly recognizes all major shortcomings in the current approaches. Such as the lack of board and business involvement and explicit sign-off to ensure commitment. The presented framework of ON2IT assigns and organises the ownership and responsibility for segment and asset risks and their measures, aka controls. These assets and controls are clearly defined in the 'classic' Zero Trust concepts of segments and transaction flows. By forcing the Zero Trust concept of *segmentation* 'up' into the boardroom strategic risk level, the alignment between risk and the required measures becomes more tangible and manageable than in existing frameworks. Mainly due to the fact that names are ascribed to assets.

A key design objective of the ON2IT Zero Trust Framework is to formalize the involvement of organization asset owners from a business perspective, yielding in more insightful interpretations of concepts such as *recovery time objectives* and *risk appetite.*

The framework obviously addresses the readiness necessities at the three separate organizational levels of cybersecurity and provides insight and control across these levels with a common language and metrics for relevant measurements. Because the effectiveness of operational measures is -near realtime- assessed in relation to the Zero Trust segments defined at the upper levels, the alignment of risk and technology can be designed and measured with greater precision. The 'relevance score', derived from traditional CIA ratings, of every individual segment, a concept integrally embedded in the methodology and Zero Trust orchestration and automation portal, drives the required controls and the required dynamic feedback on their effectiveness. This is a near real-time process. This simply cannot be a static or manual process else you cannot inform "upper" levels with proper and actual information.

Further Design Science Research based research and development for both the framework as well as the portal technology will continue and is needed in order to improve organization's security maturity, the security and risk administration, decrease risks and lower the operational cost of information security to focus on what really matters. Empirical demonstrations and evaluations of the artefact with industry professionals (CISO's, Security managers, architects) are -again- planned for 2021–2022 to continue the longitudinal research.

References

1. Betz, C.: The Impact of Digital Transformation, Agile, and DevOps on Future IT Curricula (2016)
2. Bobbert, Y., Ozkanli, N.: LockChain technology as one source of truth for Cyber, Information Security and Privacy. In: Computing Conference, London (2020)
3. CROForum. Understanding and managing the IT risk landscape: A practitioner's guide (2018). https://www.thecroforum.org/2018/12/20/understanding-and-managing-the-it-risk-land-scape-a-practitioners-guide/
4. Kumar, T.: What is the impact of distributed agile software development on team performance? Antwerp Management School, Antwerp (2020)
5. Lencioni, P.: The Five Dysfunctions of a Team; a Leadership Fable. Wiley Imprint Jossey Bass, SA USA (2002)
6. Ozkanli, N.: Implementation of Continuous Compliance; Automation of Information Security Measures in the software development process to ensure Continuous Compliance, Utrecht: Open University Press Netherlands (2020)
7. Forsgren, N.: Accelerate: The Science of Lean Software and Devops: Building and Scaling High Performing Technology Organisations. IT Revolution Press, United States (2018)
8. McCarthy, M.A.: A compliance aware software defined infrastructure. In: Proceedings of IEEE International Conference on Services Computing, pp. 560–567 (2014)
9. Bobbert, Y.: Defining a research method for engineering a Business Information Security artefact. In: Proceedings of the Enterprise Engineering Working Conference (EEWC) Forum, Antwerp (2017)
10. Hilton, M.N.N.: Trade-offs in continuous integration: assurance, security, and flexibility. In: Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering (2017)
11. ITGI, Information Risks; Who's Business are they?, United States: IT Governance Institute (2005)
12. Kuijper, N.: Effective Privacy Governance and (Change) Management Practices (Limited to GDPR Article 32) A View on GDPR Ambiguity, Non-Compliancy Risks and Effectiveness of ISO 27701 as Privacy Management System. Antwerp Management School, Antwerp (2020)
13. Kluge, D., Sambasivam, S.: Formal information security standards in German medium enterprises. In: Conisar, Phoenix (2008)
14. Siponen, M., Willison, R.: Information security management standards: problems and solutions. Inf. Manag. 46 (2009)
15. Puhakainen, P., Siponen, M.: Improving employees compliance through information systems security training; an action research study. MIS Q. **34**(4), 757–778 (2010)
16. Workman, M., Bommer, W., Straub, D.: Security lapses and the omission of information security measures: a threat control model and empirical test. Comput. Hum. Behav. **24**(6), 2799–2816 (2008)
17. Lebek, B., Uffen, J., Neumann, M., Hohler, B., Breitner, M.: Information security awareness and behavior: a theory-based literature review. Manag. Res. Rev. **12**(37), 1049–1092 (2014)
18. Yaokumah, W., Brown, S.: An empirical examination of the relationship between information security/business strategic alignment and information security governance. J. Bus. Syst. Governance Ethics **2**(9), 50–65 (2014)
19. Flores, W., Antonsen, E., Ekstedt, M.: Information security knowledge sharing in organizations: investigating the effect of behavioral information security governance and national culture. Comput. Secur. **2014–43**, 90–110 (2014)
20. Pfeffer, J., Sutton, R.: The Knowing-Doing Gap: How Smart Companies Turn Knowledge into Action. no. Harvard Business School Press (2001)

21. Bobbert, Y., Scheerder, J.: Zero trust validation: from practical approaches to theory. Sci. J. Res. Rev. **2**(5) (2020). https://doi.org/10.33552/SJRR.2020.02.000546
22. Kindervag, J.: Build Security Into Your Network's DNA: The Zero Trust Network Archit Security (2010)
23. Bobbert, Y.: Improving the Maturity of Business Information Security; On the Design and Engineering of a Business Information Security Artefact. Radboud University, Nijmegen (2018)
24. Van Niekerk, J., Von Solms, R.: Information Security Culture; a Management Perspective, pp. 476–486. Elsevier (2010)
25. Papelard, T.: Critical Succes Factors for effective Business Information Security. Antwerp Management School, Antwerpen (2017)
26. Von Solms, R., Von Solms, B.: Information security governance; a model based on the direct–control cycle. Comput. Secur. **2006**(Elsevier) Comput. Secur. **25**, 408–412 (2006)
27. Volchkov, A.: How to measure security from a governance perspective. ISACA J. **5** (2013)
28. Wieringa, R.: Design Science Methodology: For Information System and Software Engineering. Springer, Berlin (2014)
29. Johannesson, P., Perjons, E.: An Introduction to Design Science. Springer, Stockholm University (2014)
30. March, S., Smith, G.: Design and natural science research on information technology. Decis. Support Syst. **15**, 251–266 (1995)
31. Bobbert, Y.M.J.: Enterprise engineering in business information security; a case study & expert validation in security, risk and compliance artefact engineering. In: Aveiro, D. et al. (eds.) EEWC 2018. LNBIP 334, pp. 1–25. Springer, Heidelberg (2019). https://doi.org/10.1007/978-3-030-06097-8_6
32. Hevner, S., Park, J.M., Ram, S.: Design science research in information systems. Manag. Inf. Syst. Q. **28**(1), 75–105 (2004)
33. Wieringa, R.: Design science as nested problem solving. In: Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, New York (2009)
34. Straus, D.: How to Make Collaboration Work; Powerfull Ways to Build Consensus, Solve Problems and Make Decisions. Berrett-Koehler Publishers Inc, San Franciso (2002)
35. Argyris, C.: Double-loop learning, teaching, and research. Acad. Manag. **1**(2), 206–218 (2002)
36. den Hengst, M., Adkins, M., Keeken, S., Lim, A.: Which Facilitation Functions are Most Challenging: A Global Survey of Facilitators. Delft University of Technology, Delft (2005)