Model for assessing organizational security

Olli Leikas

2021 Laurea

Laurea University of Applied Sciences

Model for assessing organizational security

Olli Leikas

Safety, Security & Risk Management

Thesis

December, 2021

Laurea University of Applied Sciences **Abstract**

Safety, Security & Risk Management

Bachelor of Business Management (BBA)

Olli Leikas

Model for assessing organizational security

Year 2021 Number of pages 49

This document reports the methodology that was designed for and used in an organizational security management development project. The project was conducted in co-operation with the author and The Finnish Red Cross (FRC). The ownership of organizational security had been reassigned within the FRC and with this change had emerged the need to assess the current state of security management in a way that it also increases awareness of the topic within the organization. After further scoping, the project adopted two main objectives: Produce methodology to assess the preferred security focus areas and priorities in the target organization and produce a method to further assess the state of the focus areas.

Security of an organization is by default a very complex subject and to fully comprehend it, an understanding of the concepts of security and organization individually is needed, in addition to how security eventually integrates to an organization. The theoretical framework reviews these keywords in an extensive manner and proceeds to build understanding of how security could be arranged via a relevant management system, what perspectives of current state analysis should be considered, what can be benefitted from national security frameworks and benchmarks and how service design principles can be of tremendous value in security development work.

The core of the project implementation is described as the General Process Model. It consists of four different Phases, each of which builds on top of the previous phase. Phase 1 was designed around a workshop to define organizational security and discuss its relationship to FRC with the personnel involved in security topics. The role of Phase 2 in the process was to build on this insight and draw information from the internal operational organization using an online survey. Phase 3 aimed to reveal concrete development targets in security management. Implementation included the final workshop of the project where the gathered situation picture from previous phases was refined and deepened with a specifically designed assessment tool. Phase 4 consisted of the validation of data and the methods in different phases along with a compilation of previous elements into clear reports.

The project succeeded in generating oversight of the current state of security management and produced all its planned outputs. Key was to understand the role of the end-users in order to build sustainable paths of development that can be relevantly communicated to the organization and other interested parties. Organizational security consists of multiple areas that overlap on many occasions. With the solutions and controls of one area, an organization can affect to threats rising from another area. A thorough risk management practice helps to identify these scenarios. Usage of existing security management frameworks is highly recommended in further development as several are publicly available and they usually respond well to different organizational needs. The managerial efforts of establishing clear roles, responsibilities, action patterns and communication channels already alone can take the organization a huge leap forward as they force the organization to involve a lot of discussion on how different scenarios should be handled and with what resources. The created assessment model enables organizations to communicate the value of security and introduce the concept as a natural part of organizational management practices.

Keywords: safety and security management, assessment methodology, development project

Laurea-ammattikorkeakoulu **Tiivistelmä**

Safety, Security & Risk Management

Bachelor of Business Management (BBA)

Olli Leikas

Organisaatioturvallisuuden arviointimalli

Vuosi 2021 Sivumäärä 49

Tässä dokumentissa kuvataan organisaatioturvallisuuden hallinnan kehittämisprojektia varten suunniteltu ja siinä käytetty metodologia. Projekti toteutettiin yhteistyössä Suomen Punaisen Ristin kanssa ja sen pääasiallinen tarkoitus oli tuottaa tilannekuvaa turvallisuuden hallinnan nykytilasta niin, että projektin toteutus kasvattaisi samalla tietoisuutta turvallisuuteen liittyvistä teemoista yleisesti organisaation sisällä. Keskeisimmiksi tavoitteiksi muodostuivat metodologian tuottaminen turvallisuuden fokusalueiden ja prioriteettien arvioimiseksi kohdeorganisaatiossa sekä metodin tuottaminen fokusalueiden syvällisempää arviointia varten.

Teoreettinen viitekehys tarkastelee laajasti turvallisuutta ja organisaatiota omina käsitteinään sekä kuinka turvallisuus integroituu osaksi organisaatioita. Lisäksi se tarjoaa näkökulmia siihen, miten turvallisuuden hallintaa voidaan lähestyä systemaattisesti hallintajärjestelmän avulla, minkälaisia asioita nykytila-analyysissa on hyvä huomioida, minkälaista hyötyä voi saada kansallisista turvallisuuden viitekehyksistä sekä miten palvelumuotoilun keskeiset prinsiipit voivat luoda merkittävää lisäarvoa turvallisuuden kehittämiseen.

Metodologia pitää sisällään yleisen prosessimallin (General Process Model), johon kaikki toiminta nojaa. Se koostuu neljästä erillisestä vaiheesta, jossa jokainen rakentuu aina edellisen vaiheen pohjalle. Ensimmäinen vaihe määrittelee workshop-ympäristön avulla organisaatioturvallisuutta käsitteenä turvallisuuden koordinaatioryhmän kanssa. Toinen vaihe jatkaa ymmärryksen rakentamista muulle sisäiselle organisaatiolle suunnatun verkkokyselyn avulla. Kolmannen vaiheen tarkoitus oli paljastaa konkreettisia kehityskohteita turvallisuuden hallinnassa tähän tarkoitukseen suunnitellulla arviointityökalulla. Toteutuksellisesti tämä tapahtui projektin viimeisessä workshopissa jälleen yhdessä turvallisuuden koordinaatioryhmän kanssa. Neljännessä vaiheessa projektissa tuotettua dataa ja metodologiaa validoitiin erilaisten työkalujen avulla sekä tuotettiin dokumentaatiota loppuraportointia varten.

Projekti onnistui täyttämään asetetut tavoitteet sekä tuottamaan suunnitellun prosessin mukaiset lopputuotteet. Olennaista oli alusta alkaen ymmärtää loppukäyttäjien rooli kehitystyössä, jotta turvallisuuden kehittäminen yleisesti rakentuu kestävälle pohjalle ja sitä on mahdollista kommunikoida relevanteille sidosryhmille. Organisaatioturvallisuus kostuu useista eri osa-alueista, jotka monissa tapauksissa risteävät keskenään. Yhden alueen ratkaisuilla on mahdollista vaikuttaa riskeihin, jotka saattavat nousta joltain toiselta alueelta. Vahva riskienhallintaosaaminen edesauttaa näiden tilanteiden tunnistamisessa. Tulevaisuuden kehittämistä varten on erityisen suositeltavaa hyödyntää olemassa olevia turvallisuuden hallinnan viitekehyksiä, joita on useitakin vapaasti saatavilla ja jotka pääsääntöisesti vastaavat hyvin organisaatioiden eri tarpeisiin. Hallinnollisten elementtien, kuten roolien, vastuiden, toimintamallien ja viestintäkanavien, kehittäminen voi jo itsessään viedä organisaatiota merkittävästi eteenpäin, sillä ne vaativat aktiivista dialogia erilaisten tilanteiden hallinnasta sekä niissä tarvittavista resursseista. Tässä projektissa tuotettu arviointimalli antaa organisaatioille mahdollisuuden kommunikoida turvallisuuden luomaa arvoa sekä esitellä sen soveltumista luonnolliseksi osaksi normaalia organisaation johtamista.

Asiasanat: turvallisuusjohtaminen, arviointimalli, kehittämisprojekti

Contents

1 Introduction

This document reports the methodology that was designed for and used in an organizational security management development project. The project was conducted in co-operation with the author and The Finnish Red Cross (FRC). This report consists of introductionary parts that present the FRC, original project scoping, premise and objectives; theoretical context parts that describe the most relevant terminology and frameworks required in the project; implementation phase parts which present the what, why and how things were done as well as reflect on their success; evaluation part that takes into account the project in whole and analyzes its triumphs and shortcomings; and conclusion part that compiles the gained insight and offers closing remarks.

1.1 Client Introduction

The Finnish Red Cross is a humanitarian aid and disaster relief organization operating on national and international environments. It is the only national governmental organization that can be a part of the international movement of the Red Cross and the Red Crescent. The FRC has a special legal status that is governed by the Act on the Finnish Red Cross and the Presidential Decree on the Finnish Red Cross. The primary mission of the FRC is to support and assist national authorities in times of both peace and war and during armed conflicts in order to promote human well-being. In a wider context their mission is to protect life in all circumstances relying on their seven fundamental principles: humanity, impartiality, neutrality, independence, voluntary service, unity and universality. To fulfill its mission the Finnish Red Cross engages in a variety of activities such as providing assistance and resources in emergencies, offering first-aid services and training, providing support for immigrants and refugee and asylum seeker reception, fundraising and campaigning, operating blood services, second-hand stores and youth safehouses, and coordinating the voluntary rescue service known as VAPEPA. (Finnish Red Cross 2021a; 2021b.)

The national movement must be directed by a central body. This derives from the Statutes of the International Red Cross Article 4, Conditions for Recognition of National societies. (Finnish Red Cross 2020.) According to the Presidential Decree (Finland 2017) the central body of The Finnish Red Cross consists of the board of the organization, Secretary General, central office and the institutions founded to support the achievement of Finnish Red Cross' mission. The whole domestic organization also includes regional districts and local branches. The highest decision-making power lies in the General Assembly which takes place every three years. (Finnish Red Cross 2021b.)

The development project was conducted with, and limited to, the central office of the central body, which coordinates the operations of the FRC both nationally and internationally. Responsibility of the central office is to develop the organization, state level co-operation with public sector authorities, national campaigns and influencing, and international co-operation. (Finnish Red Cross 2021a.)

1.2 Project Premise & Objectives

The project originally initiated from a dialogue with the FRC representative, where it was brought to attention that the ownership of organizational security had been reassigned within the FRC with the intention to develop the domain in the future. For the ability to effectively address different security matters within the organization, there was a need to gain oversight of the current state of security first. The question in general level was how to assess the organizational security so that it brings awareness to the organization involved. The assessment should expand the toolbox for security development, consider how the organization could be connected in the assessment process and ensure that the assessment could be reproduced in the future.

The positioning of non-governmental organizations, and particularly the Finnish Red Cross, as a vital supportive function to national security is promoted in a number of strategies and publications by the public sector authorities. Especially developing resiliency within the society, providing valuable surface area to national and international networks along with the insight to the society's ground level status are what the authorities rely on. (Prime Minister's Office 2017.) This standpoint alone would have made a well justified case for a security development project that targets the FRC organization itself. By increasing the maturity in the level of security, the organization communicates reliability and responsibility while the same time increasing their service value.

Observations and discussions indicated that coordinated management regarding organizational security might currently be relatively immature in the client organization. Documentation and guidelines regarding security did exist, but they considered more of the general risk approach of the organization, security of the volunteers during operations, ethical guidelines, and statements on data protection. As a whole they did not consider a way to manage the security of the organization itself. This, however, did not imply that the elements of organizational security were necessarily missing, but they might be addressed on a more reactive basis without a connection to systematic management procedures. Nevertheless, these notations seemed to be accompanied with minimal resourcing and low possibility to prioritize development initiatives in the short-term future, which further directed the interest and scope of the project towards improving security management.

These observations in mind, the scoping sessions and dialogue with the FRC led to a proposal of a development project that would consist of the production of the needed oversight from the perspective of the current state in organizational security management. The model would be created for, and tested in co-operation with client, with intention to produce a generally applicable framework for other organizations as well. All client specific internal information produced in the implementation phases would therefore be left out of this public project report.

The thesis report discloses the methodology used, tools created and validation of their success regarding the project. The aims, outputs, and the role of the outputs for the project were planned as follows:

1. Produce methodology to assess the preferred security focus areas and priorities in the target organization.
2. Produce a method to further assess the state of the focus areas.

	Development project output	**Role**
1.	A general process model for repeatability and validation (Assessment methodology, Aim 1)	Sequencing of implementation
2.	Tools, a questionnaire and compilation tables, to specify organizational security definitions and common threats in relation to FRC	Input for Phase 1 implementation
3.	A survey to measure current “security pulse” from key functions	Input for Phase 2 implementation
4.	A checklist -type of security management assessment tool to gain more insight of security focus points (Aim 2)	Input for Phase 3 implementation
5.	Data and methodology validation tools	Input for Phase 4 implementation
6.	A compiling report including follow-up activity suggestions	Presents results of implementation (FRC)

Table 1: Targeted project outputs

2 Theoretical Background

Security of an organization is by default a very complex subject. According to the Confederation of Finnish Industries (CFI) however, the central function of organizational security is rather clear. It intends to enhance the organization's ability to provide its products and services and thus establish and develop the organization's role as a part of its environment. Security management is considered a natural part of general management activities and bring the leadership tools that aim to safeguard the continuity of operations, enable normal justified risk taking, ensure compliancy with certain regulative requirements and restrict unnecessary disruptions from vulnerabilities in the organization. (Confederation of Finnish Industries n.d.) But to fully comprehend the subject, there must be an understanding of what is meant by security and organization in the first place, and how security as a concept integrates to an organization.

Over the last decades there has been an upshift regarding the meaning and emphasis in organizational risk management that also impacts the management of organizational security. It shows in the change of emphasis from technical elements of security towards the management of complexity, uncertainty and ambiguity. The organizations must consider the increasing risks that the new information and cyber environments produce, the risks of being more interconnected within the supply chains and other risks that might not be direct but effect the balance of operational environment such as terrorism and environmental damage. Also, the meaning of contractual and responsibility related liabilities has been realized with the increased understanding of their effect to the quality of production along with the effect to reputation. Not to mention that in addition to the new emerging risks, the organization must still manage with the traditional strategic, financial and operational risks. (Lanne 2007.)

2.1 Key terminology

Security is "multidimensional in nature and diverse in practice which leads to a difficulty in providing an encompassing definition for all applied domains in the field" (Brooks 2010). From a standardized vocabulary perspective, security as a concept refers to a state where threats and risks of the defined scope are manageable. It can also mean an activity or a set of activities that aim to control the **threats** and **risks** within scope, but as well a feeling of being in control of the threats and risks. Security considers the intentional malicious attempts to inflict harm and other damage, including protection against violence, crime, theft, and fraud for example. However, it should be accompanied with non-intentional element of **safety** that includes the same preface as security, but where the events originate in contexts such as accidents, emergencies, and mistakes. (The Finnish Terminology Centre 2017)

Literature portrays the necessity of safety and security for the functioning of societies. As far as to the statement that without these elements there is no freedom, no happiness and also

no prosperity. (Jacobs et al. 2020.) As described by Bibi van den Berg, Pauline Hutten and Ruth Prins, and edited by Jacobs (et al.), safety and security are the fundamental drivers for living beings. Beginning with primary safeguards, such as having shelter, access to food and drink to sustain physical health, and being protected from violence or natural disasters. Secondary and tertiary security elements consider for example the societal bonds without which life would be solitary or poor, and having a sense of belonging in the form of social relationships with others, such as family and friends. This includes the sense of experiential security, an idea that one can develop and maintain a sense of identity within a safe and stable environment. One can also approach safety and security from an objective or subjective angle. Objective side referring to the fact that if secure and safe, things are not actually, factually threatened. Subjective in contrast refers to the mental state of humans where safety and security is a feeling that balances, controls or erases the fear of a threat. (Jacobs et al. 2020.)

If taken apart, security recognizes the existence of threats, risks, vulnerabilities, assets and incidents. **Threat** is defined as the potential cause for, and/or a possibly occurring harmful event or event progression. It is the uncertain negative derivate of the risk variable. As opposed to a **possibility**, the positive counterpart. (Finnish Standards Association 2021; The Finnish Terminology Centre 2017.) **Risk** on the other hand is an effect of uncertainty on objects, where the effect is a deviation from the expected. The risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood. (Finnish Standards Association 2021.) **Vulnerability** is an exploitable weakness or predisposition to threats for example in processes or systems that enables the realization of a threat, be it intentional or unintentional, man-made or product of the environment, or something else. (The Finnish Terminology Centre 2018.) **An asset** refers to the target of protection methods and is generally defined to be anything that has a meaning and value to an organization. It typically includes categories such as personnel, information, technologies, premises, property, and stakeholders. (The Finnish Terminology Centre 2018.) **An incident** is an event that can or could lead for example to a disruption, loss or an emergency. From a security point of view, an incident usually has different thresholds that vary depending on the organization and the type and severity of the event, and have different meanings and protocols attached to them. An incident might turn into a disturbance, crisis or even a catastrophe or disaster. (Finnish Standards Association 2021; The Finnish Terminology Centre 2017.)

If building high-level context, then security integrates to the concepts such as comprehensive security, continuity management and risk management. **Comprehensive security** has a couple of different meanings where one addresses the security as a perception of what it consists of, and the other as a concept of how a nation, for instance, should approach security in the society. It encompasses all such questions related to security and safety that

could have a significant negative impact on population or society and refers to a wider security understanding, where applicable contexts vary from traditional military threats to other threats such as climate change, epidemics, terrorism, cyber-attacks and drug trafficking. (The Finnish Terminology Centre 2017.) **Continuity management** is a planned set of strategic and operative processes and methods to identify critical threats to the organizations' operations, assess their impact to each stakeholder and react and recover in the case of different incidents and disturbances. It emphasizes resiliency and building the ability to continue providing service on an acceptable level despite, and during, possible disturbances that might last an indefinite amount of time. (The Finnish Terminology Centre 2017.) **Risk management** can be considered the fundamental idea behind security, but in general it also refers to any systematic activity to identify the risks in a defined scope, assess the possible threats and possibilities, implement controls and safeguards against threats and take advantage of possibilities, monitor implementation and follow-up with corrective action. (The Finnish Terminology Centre 2017.)

When examining the meaning of only an **organization**, a modified dictionary definition would be a group of people who work together in an organized way for a shared purpose, utilizing a set of resources such as facilities, information and technologies. (Cambridge Dictionary n.d.) While rather clear and encompassing, this definition, however, lacks much of the depth that organizations embody when examining theoretical studies. For instance, the way an organization is perceived and understood is also meaningful, as it significantly affects to the conclusions that can be made about its leadership and management in addition to how its activities can be influenced. Nieminen (et al. 2017) presents a rather interesting way of approach that bases on the organizational studies of Gareth Morgan from 1977, the Images of organization. Similarly to Brooks' view on security and safety (2010), this theory proposes that organizations are multidimensional and diverse in nature. Organizations are considered as systems that should be reviewed through different lenses, for which eight possible perceptions are depicted via Morgan's metaphors. These metaphors propose that organizations could be seen as a machine, an organism, a brain, a culture, a political system, a psychological prison, an instrument of dominance and/or as a stream or transformation. An organization usually encompasses elements of more than one of these. (Nieminen et al. 2017.)

A machine incorporates the idea of an organization being a rational system, built for a certain purpose that seeks maximum efficiency. It includes a strong segregation of duties such as planning and production, with a definitive division of responsibilities. **An organism** introduces the concept of systemicity. It recognizes the interconnectivity of smaller partial systems and technical environments in relation to the more comprehensive ecosystem. **A brain** sees the organization as an information processing, communicating and decision making system. The organization proactively observes and anticipates its environment, develops an

ability to question, challenge and alter its base assumptions and default activities, but also enable the development of strategic directions and complementing methodologies. **A culture** reviews for instance how the members of an entity interact with each other and what they consider important. In whole it encompasses all organizational interaction in its relevant contexts. In the deepest layer, culture acts as the subconscious of an organization where the characteristics of an organization have generally been acknowledged and accepted as is, in good or bad. The middle layer regards the outspoken elements of culture, such as values, strategies, mission and vision. The surface level shows in the processes and composition or structure of the organization, in the common language and premises design for instance. **A political system** acknowledges that power and politics are inseparable part of all organizations. It refers for example to the accessibility on resources, decision-making abilities, personnel networks along with interests and conflicts management. **A psychological prison** describes an organization that has become blind to the change in environment and the need for the organization to change as well. It can be considered a sort of a tunnel vision where ability to focus on important things is compromised as the overview in general has critically narrowed. **An instrument of dominance** raises the issue where organizations might not have completely good intentions. Taking advantage of the personnel is a negative example of dominance. Another example, that might be positive or negative depending, is to gain so much control for instance in international markets that it is possible to impact the decision making in global economies. The eighth perception of an organization as **a stream or transformation** refer to a learning organization that interacts with the impulses of the environment and the people, develops more capabilities to provide its services and live in the constant change. (Nieminen et al. 2017.)

While Brooks (2010) debated on the complexity of security and Nieminen (et al. 2017) recognized the many perceptions of an organization, theories of learning organizations that consider systemic thinking could provide context for developing effective organizational security management for their similarities in the nature of the fields. Systematic or systems thinking is understood as the key in countering and facilitating the complexity and foundational uncertainty of the world. Security on the other hand aims to mitigate the effects of negative outcomes deriving from uncertain and complex events. Robert Flood (1999) reviews Peter Senge’s Fifth Discipline that could provide interesting possibilities and applicable theories for developing security via organizational theory studies. The Fifth Discipline remarks five necessary disciplines for learning organizations: personal mastery, mental models, shared vision, team learning, and systems thinking. Flood also mentions Ludwig von Bertalanffy's open systems theory, Stafford Beer's organisational cybernetics theory, Russel L. Ackoff's interactive planning theory, Peter B. Checkland's soft systems approach theory, and C. West Churchman's critical systemic thinking theory as good perspectives of reflection when developing organizational capabilities. (Flood 1999.)

Organizational security as a concept considers all security and safety related activities of an organized group of people, that regard protecting its personnel, information, premises, property, technological infrastructure, and environment for instance. It includes the management of uncertainty, threats and risks in the spirit comprehensive security ideology. (The Finnish Terminology Centre 2017.) This definition along with the introductionary discussion of the theoretical background about the security of organization gives a rather powerful stand on viewing organizational security first and foremost as a holistic management discipline at the high level.

By default, organizational security is as divergent concept as security and organization individually. There is, and has to be, as much variance in the arrangements, focus and priorities of organizational security as there are organizations. The different resources, structure, operational fields, interconnectivity, culture and the different applicable risk categories require an individual approach from each entity. For instance, the operational field of the organization also dictates what areas from security perspective should or must be considered. Most elements are relatable or directly regard all organizations, such as premises security and occupational health and safety and information security but understandably in different scales. An organization that specialises in producing goods to multiple markets should probably focus on the security of production and facilities with a relatively high budget, while a consultant firm of less than 10 people might want to secure its personnel and information for example and can make reasonable arrangements already via policies and guidelines only. In organizational security the challenge is to compile a comprehensive situation picture from the complexity, but also to coordinate the security activities of different fields into an effective body that serves the general interests of the organization. (Lanne 2007.)

2.2 ISO 22301:2019 - A Security Management System

Organizational security management is an integral part of building a more mature security posture within an organization. The mapping of organizational threat landscape and their impact assessment as well as placing necessary risk management controls and implementing other related activities are key in successfully increasing the maturity in the organizations' security level. CFI promotes the approach of layering security activities, from managerial elements to more technical functionalities, and active inclusion of the relevant stakeholders to the process. While the technical side is important, it is at least equally necessary to promote the intangible elements of awareness, culture, and the communication of these matters. (Confederation of Finnish Industries n.d.) The adoption of secure practices and culture within organization requires commitment and active participation to a common goal. These are incremental to ensure observation and identification of threats, sharing of

necessary information to relevant people, plan development initiatives and maintain situation awareness. (Lanne 2007)

A standardized management system allows the organization to conform with widely accepted best practices, communicate the level of maturity easily to its interested parties even on international platforms, but also adopt field specific practices as a part of the management system by adjusting the scope. The development project orientates the FRC to take initial steps in terms of understanding the contexts of the organization and adjusting the scope for future development programs. Therefore, it was logical to provide insight on a standardized management system, as these themes can be considered a prerequisite for building conformity with a standard. Also, the CFI promotes the usage of different international standards in the management of organizational security. (International Organization for Standardization 2019, Confederation of Finnish Industries n.d.)

The International Organization for Standardization (ISO) standard, ISO 22301:2019 for security and resilience - a business continuity management system (BCSM), has a great general applicability considering this project. At the time of the development project, ISO also maintained a free read-only version of the standard on their website, making it easily accessible as well. In addition to the ISO 22301:2019, and according to the Confederation of Finnish Industries (n.d.), widely used management systems that are directly linked to organizational security are, for example, the ISO 9001 for quality management, the ISO 27001 for information security and the ISO 45001 for occupational health and safety.

All ISO-based management systems follow a similar component structure while promoting certain field specific characteristics and apply the Plan (establish), Do (implement and operate), Check (monitor and review) and Act (maintain and improve) cycle to ensure the effectiveness of the system. The ISO 22301:2019 document emphasizes the importance of understanding the organization’s needs and current profile, the necessity for establishing business continuity policies and objectives, operating and maintaining processes, capabilities and response structures for ensuring the organization will survive disruptions, monitoring and reviewing the performance along with the effectiveness of the BCMS and continual improvement based on qualitative and quantitative measures. Via a business continuity management system an organization could improve its ability to withstand uncertainty and add value to its operational and supporting processes. This is described in more detail in the figure 1 below, which proposes that implementing the standard means that the organization proactively advances its maturity considering the perspectives of business in general, financial aspects, interested parties and internal processes. (International Organization for Standardization 2019.)

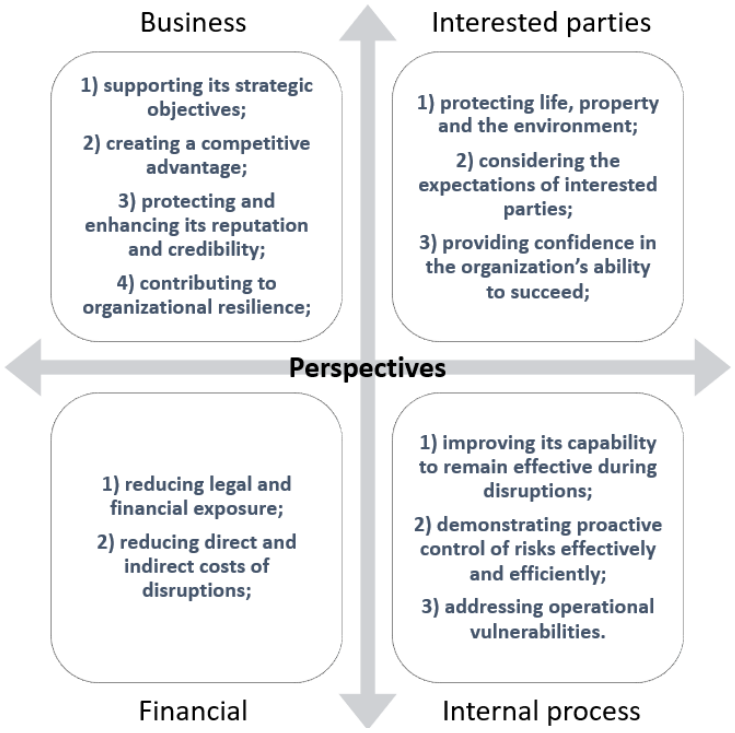

Figure 1: Perspectives of advancement when implementing ISO 22301:2019 (International Organization for Standardization 2019)

2.3 Current state analysis

The primary objective of the methodologies used in the project is to increase understanding of the current situation in order to make defendable decisions about the course of security development in the future. Generation of a valid **situation picture** on a topic, i.e. the combination of various sources to gather a holistic view about an event and its progression with contextual background, is incremental in supporting timely and accurate decision-making. It is also needed to provide general **situation awareness** and understanding of possible continuums to justify decision-making. (The Finnish Terminology Centre 2017.)

According to the CFI principle of layering organizational security, also the analysis of current state should be layered. Uchendu (et al. 2021), for instance, recalls that considering security management and culture the most influential factors, i.e. the elements that should be kept track on and under consistent revision, are management support, policy and procedures, and awareness. In addition, linkage to the general organizational culture and change management should be considered. Questionnaires and surveys are the most trusted or used tools in the collection of such information for a high-level situation picture. Whereas Wang (et al. 2018) required a more pragmatic view on the current state of work safety in China by carrying out a statistical analysis of accidents and occupational diseases in recent years in China. This was considered to be an essential part to form effective action plans and make decisions on future

tasks and development. Casino et al. (2019), remind that increased interconnectivity reveals the need to maintain a holistic view on the whole. This kind of perspective could for example be acquired with a systematic review and thematic content analysis of literature. Similarly to the CFI perception of the security domain, the blockchain technology studied by Casino (et al.) either is not a solution for just one thing but can be used in a number of different contexts. Understanding of the connections and contexts allows for the ability to identify gaps and focus points, which are needed to make defendable choices in development work from a practitioner point of view. (Casino et al. 2019.) Stenberg (2017) emphasizes the meaning of understanding the experiences of different parties regarding security, for they significantly impact the security culture in general and how the culture correlates to attitudes, values, and perceptions of security. The importance of this view is in line with the preceding theoretical findings that suggest that security culture might have a rather critical role in security management, but also management in general. Additionally, Stenberg provides a valuable benchmark in how the data should be used for multiple different purposes. For example, in his diploma work the survey results provided the required insight on current state, but they were additionally used with a behavioural theory to gain a perspective on possible causes of the current state. (Stenberg 2017.)

In general, a key tool to successful security management is the understanding and proper use of information, including consistent assessment of current state. Information is needed to broaden management's vision and ability to make decisions, increase effectiveness of security activities, assist in the planning for future security requirements and budgets and to effectively reduce risks to an acceptable and manageable level. (Sennewald 2011)

2.4 Domestic security benchmarks

Finnish national security frameworks and best practices offer a reliable way to compare one's posture against regulatory compliancy and advanced levels of maturity from the perspective of society. They are designed to increase the resilience in the nation, which after scoping and scaling are highly useful to any organization for developing their organizational security management. Notable public frameworks and benchmarks are the municipality continuity model **KUJA** developed by the Association of Finnish Municipalities, the national security auditing criterion **KATAKRI 2020** maintained and developed by the National Security Authority (NSA) and the **VAHTI-guidelines** of Digital and Population Data Services Agency for addressing digital and information security in the government organizations. All of these frameworks serve a great developmental purpose for their complementary nature towards each other, connections to international standards and regulation and availability as free publications. In addition, they integrate well to the theoretical framework of the Confederation of Finnish Industries and their organizational security model, which as a concept is further introduced in chapter 3.1.

KUJA model came to life in a joint project between the Association of Finnish Municipalities and National Emergency Supply Agency (NESA) that aimed to support and develop the preparedness and continuity related capabilities in the municipality sector. The intention was to harmonize the basic principles and methods along with applicable tools to offer the municipalities a purposeful and efficient way to follow through their regulative duties in preparedness and enhance the quality of operations. From this framework the project reflects especially on the KUJA tools. The primary set-up includes an action or reporting card for incident management purposes, a speed test to evaluate the state of continuity and full scale current state and maturity assessment tool. KUJA has been built on five modules relevant to continuity: leadership and management, processes, anticipation and planning, incident and crisis management, and co-operation. (Association of Finnish Municipalities n.d.; Association of Finnish Municipalities 2019a.)

KATAKRI 2020, the current and fourth version, is a product of continuous iteration and development. The first version was completed in 2009 as a part of the government's program on internal security. The third version of the auditing tool shaped the structure and content to focus primarily on the security of classified information. From the beginning, KATAKRI has been developed in close collaboration of the public, private and third sectors which has shown in the additional value it has produced over the years especially considering reputation in information security. In itself, the audit tool does not present unconditional requirements. However, KATAKRI is based on legislation and internationally binding information security requirements. It is divided into three sections that cover the modules of security management, physical security and technical information security. The core principle regarding assessment of performance in any of the modules is systematic and well-rounded risk evaluation. (National Security Authority 2020.)

VAHTI-guidelines are a collection of instructions and requirements to ensure information security in public organizations. They are an exhaustive approach to security in general and they do, for example, promote the implementation of the Security Strategy for Society, the Government Resolution on Security of Supply, and the National Information Security Strategy. The guidelines are also used in many instances as a reference for KATAKRI assessments. The VAHTI collection aims to improve the reliability, continuity, quality, risk management and contingency planning of central government functions, but can be used in other organizations as well. They address information security from management point of view and technical aspects, but also provide advice on arranging personnel and premises security and continuity management for instance. (Digital and Population Data Services Agency 2021.)

By applying the guidance and principles of these frameworks, an organization should be well able to construct a mature organizational security environment that is also in line with international standardization. VAHTI-guidelines are probably the most comprehensive singular

source of instruction. KUJA can be used as a hardening method and validation of the capabilities considering continuity management. Same goes for KATAKRI 2020 that reinforces the elements of security management and the technical aspects of security. The CFI security model provides context to other perspectives in modern organizational security thinking and helps to comprehend the diversity and extensiveness of the field.

2.5 Service Design

Service design thinking and doing benefits security development for many reasons and the approaches of this discipline were deeply embedded into the methodologies of the project implementation. In general, the approach was also a good fit to the nature of FRC as a major service provider. The core strengths of the Finnish Red Cross are the ability to react quickly, ability to act independently from the authorities and provide critical services that enable the management of difficult situations which are characteristics that need to be preserved and considered in security development. (Prime Minister's Office 2017.)

Historically, service design as a concept originates from marketing studies and has benefitted from its long maturation period, especially in the development of the toolbox used within the field. Generally, there has always been a need to appropriately design all the components of a service for the targeted markets. Now with the rise of service design frameworks that have cross-pollinated between different design disciplines such as industrial design and interaction design, the applicability of the methodologies for any organization is tremendous. (Morelli 2021.)

Service design is about blueprinting, i.e. designing and codifying the sequence of actions, a service performance. The design frameworks can be analyzed from a number of positions. One can focus on the organization of operational processes and the coordination of backstage of services (the design of facilities, servers, equipment and other resources), client perspectives and the interface between clients and service providers, the visualization, formulation or orchestration of service solutions as well as services as experiences that happen over time and that need to be organized through a sequence of interactions between service providers and customers. (Morelli 2021.) The essential idea in service design is to create or improve the value generated by an organization. It adopts the setting of a design process and combines it with an active, iterative approach and tools borrowed from user experience, software development and branding among others. As a discipline it is all about solving the right problem by framing the problem or opportunity the right way and usually the beginning phase of service design investigates the needs of the user or customer. From the research angle, service design is optimal when a good mixture of methods is used, varying from desk research and observations to surveys, interviews, and workshops. Another pro for using service design in combination with working life, is that it is an intensely practical,

pragmatic and consequently inherently holistic approach. In order to create or improve value, there must be a consideration of the end-to-end experience of multiple interested parties and a way to make it profitable, regarding the actual business needs of the organization and the appropriate use of technology. (Stickdorn et al. 2018.)

In the service design, the nature of the actual need impacts on how to proceed and address different development ideas. For instance, there might be a need for a redesign of the service, and due to the nature of the market, it is not expected to change in the short time. Or to the contrary, possibly because of changes in demand or frequent innovations in service technology, it is necessary to continuously redesign the service and its production and management processes. Consequently, the latter means that another level of processes is required, designed to provide a continuous capability for the redesign and generate innovations to keep the service competitive. Service design has the most usability when approached with a hierarchical top-down perspective, i.e. selected components are progressively designed in increasing levels of detail and building on previously defined components and processes. This should assure a systemic, consistent, and efficient global design. Alternatively, however, it is possible to proceed with individual "local designs," without having a global business design on the background and a link to previous decisions of structure and performance. This situation might arise when priorities, timing, resources, and other restrictions affect the justifiability of a more systemic and thorough approach. (Barros 2017.)

Morelli (2021) explains that service design requires a number of capabilities, some of which are typically personal (e.g. empathy, the capability to understand logical or social contexts), while others are generically professional (e.g. business capabilities, organisational capabilities, sensitivity to aesthetics and form). In a wider context, these include capabilities to research contexts, provide perspectives on possible future situations, and structure design processes. These capabilities are directly linked to the preceding theories of constructing organizational security and building situational awareness through current state analysis. Additionally, similarly to the concept of individualizing organizational security management per entity, the same capability will produce different effects and support different strategies depending on whether the designer is supporting people's interaction in the value creation context, designing the structure of a service, or contributing to policies or strategies that aim to change the institutional context.

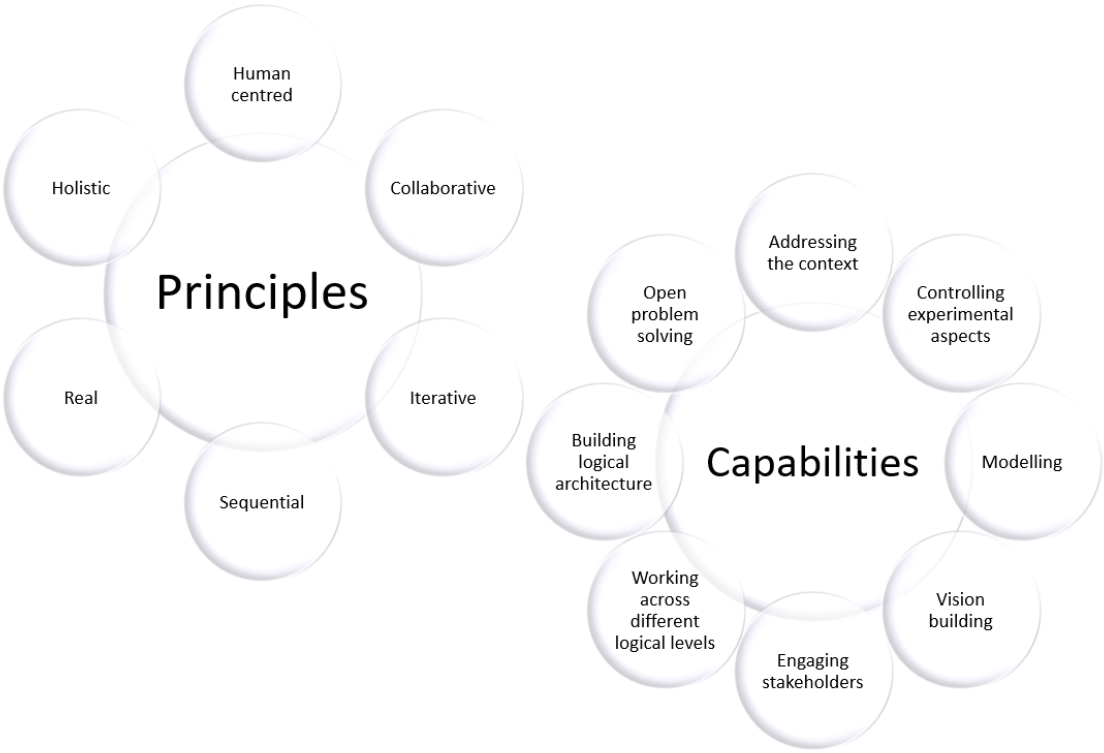

Figure 2: Principles and required capabilities for effective service design (Stickdorn et al. 2018; Morelli 2021)

The principles (Stickdorn et al. 2018), and the specific required capabilities of service design (Morelli 2021), gathered to figure 2 above, communicate the essence of why the discipline is so effective. When service design is **human-centred**, it considers the experience of all the people affected by the service; when it is **collaborative,** it actively engages stakeholders of various backgrounds and functions in the service design process; when it is **iterative,** it is an exploratory, adaptive, and experimental approach, iterating toward implementation; when it is **sequential,** it visualizes and orchestrates the service as a sequence of interrelated actions; when it is **real,** it researches needs in reality, prototypes ideas in reality, and provides evidence of intangible values physical or digital reality; and when it is **holistic,** it produces services that sustainably address the needs of all stakeholders through the entire service and across the business. (Stickdorn et al. 2018.) When a service designer **addresses the context**, there is an identification and response to relationships between a solution and its context. **Controlling experiential aspects** requires empathising with people and addressing experiential features of possible solutions. **Modelling** needs simulating, visualising and experimenting with possible solutions before all the information is available and using a form to embody ideas and communicate values, while **vision building** regards to imagining feasible, possible and desirable futures. **Engaging stakeholders** means that the designer is proactively initiating and facilitating participatory co-creation processes. In addition, the

designer must be able to shift from operative levels to different levels of abstraction, i.e. **work across different logical levels** as well as articulate or identify logical structures to frame problems and creative activities, i.e. **build logical architecture**. Eventually the capability of **open problem solving** enables the designer to identify solutions across different logical domains and within uncertain and ambiguous contexts. (Morelli 2021.)

3 Implementation

The following chapters cover the different phases of implementation and the methodology designed for and used in the development project. Table 2 presents the assessment methodology, the General Process Model, in one table with the description of method, required inputs and produced outputs. The subsections offer deeper insight on each phase, to the matters of why such steps were designed, how the methodology was implemented and how successful the results can be considered, using reflective writing. The reflective nature of these sections allow to build reasoning and evaluation of success, while also recognizing the author's role in the implementation and therefore enabling a more robust dialogue for each subsection.

The phases of implementation align with the PDCA cycle of the ISO 22301:2019 standard. It is intended that with the methodology used in this project FRC, for instance, can achieve a certain baseline for future conformity with the standard, if considered desirable. The project provides insight for the clause 4 of the standard; the requirements necessary to establish the context of the BCMS applicable to the organization, as well as needs, requirements, and scope. In addition, via the targeted project outputs, the project should provide documented insight and justification for the purposes of building a policy statement that can be approved by the leadership (clause 5) and used in establishing meaningful strategic objectives to guide the development (clause 6). The project also should do its own part in operational sense by building competence to understand security related terminology and thus enabling a more consistent communication in the future, raising awareness within the internal organization, and creating documentation (clause 7). By invoking the internal organization to take part in the form of a survey, the project additionally has a platform to take into account the operational units' perspectives and needs of security as required in clause 8. Finally, in accordance with clause 9, through the workshop and survey tools, the project enables the design of relevant metrics to assess development. (International Organization for Standardization 2019)

Implementation phase	Contextual inputs for implementation	Technical inputs for implementation	Implementation methodology	Outputs of implementation
Phase 1: Defining security	Reference framework of security terminology (for instance the CFI security model in this project)	Tools, a questionnaire and compilation tables, to specify organizational security definitions and common threats in relation to FRC	Structured workshop with organization's security coordinators	Documented personal views of the security coordinators Documented common view of the security coordinators Documented preferred scope of development with initial connections to own environment
Phase 2: Identifying organizational priorities	Reference framework of security terminology Phase 1 Outputs	A survey to measure current "security pulse" from key functions	Online survey to the FRC internal organization	Documented and analyzed views of the organization on safety and security Documented focus areas for organizational security development
Phase 3: Focusing and deepening the insight	Reference framework of assessment Phase 1 & 2 Outputs	A checklist -type of security management assessment tool to gain more insight of security focus points	Structured workshop with organization's security coordinators	Documented security management current state of the focus areas

Phase 4: Validating, concluding & reporting	Reference framework of validation Documentation of previous phases	Data and methodology validation tools	Desktop assessment and compilation of project phases and results	Documented validation of data and methods Compiling project reports with follow-up suggestions

Table 2: General Process Model

3.1 Phase 1: Defining security

A well-designed professional lexicon improves communication between different parties and prevents unnecessary misunderstandings. It is incremental in building an accurate and timely situation picture that can be communicated to relevant interested parties. (The Finnish Terminology Centre 2017.)

The first phase in the process was designed to level the common ground in terminology considering the Confederation of Finnish Industries' definitions of the different areas of security and their relationship to FRC, from the perspective of the security coordinators. The CFI has developed and maintained a nationally recognized organizational security model for a long time that examines the security field through nine different security areas: personnel security, property and premises security, rescue safety, production and operational security, environmental security, information security (including cyber security), transgression and incident management, preparedness and crisis management, and occupational health and safety (OHS). The central function of organizational security model is to enhance the organization's ability to provide its products and services and thus establish and develop the organization's role as a part of its environment. Security management is considered a natural part of general management activities and bring the leadership tools that aim to safeguard the continuity of operations, enable normal justified risk taking, ensure compliancy with certain regulative requirements and restrict unnecessary disruptions from vulnerabilities in the organization. (Confederation of Finnish Industries n.d.) Security is not something static but rather something that is shaping in a constant dynamic with the environment and the actors in it. This means that the focus areas differ with every organization, even though there are many areas that are generally applicable. For these reasons the CFI model was adopted as the reference framework of this phase, and specifically the categorization of organizational security to different areas along with their definitions and content examples.

Group discussion or group interview is a qualitative data collection method that seeks to find out whether or not a consensus can be reached via discussion on a certain topic. The interviewer's role is to facilitate the discussion. (Finnish Social Science Data Archive 2021a.) Involving the security coordinators to incorporate their views on security was essential to build enough layering to the general process model which made the use of this method fairly justified. The group interview in the workshop however was built on a more structured form rather than allowing a completely free discussion. This decision was made to enable a reasonable timeframe, an hour and a half, for the session that can be considered by the participants as a normal stakeholder meeting instead of a long disruption to working ability. The structured form allowed a certain standardization, objectivity, and measurability in the results but also the speed in response time. The structure included an online questionnaire and in advance prepared compilation tables for cross referencing. The Likert scale in answering options of the questionnaire allowed the personal perceptions to be recorded. (Finnish Social Science Data Archive 2021b.)

Figure 3: Workshop process chart, Phase 1

The workshop was implemented on an online platform, Microsoft Teams, to enable flexibility and ease of access for participants, but it also enabled an efficient way of working according to the workshop process chart above in figure 3. Half an hour of the workshop was reserved for introductionary discussion with the group and the actual workshop was conducted within an hour. The intention of the online questionnaire in the beginning was to introduce the participants to the security framework and establish the accepted reference of concepts. From my perspective as the facilitator the following process took place: To begin to establish the baseline, I asked each participant to open a link to the online form while presenting the same time on the screen the definitions of the CFI security model. Upon each of the nine definitions, the participants provided their insight via two questions as presented in Table 3 below. The key word was intuition and to avoid unnecessary hesitation as a facilitator my role was to maintain a rather fast tempo. This method made it possible for the group to easily address how they stand on the given definition using their current understanding of the organization and their areas of responsibility.

Security area statement	Assessment				
Considering the nature of the operation, the organization covers the contents of the security area at least sufficiently.	Fully agree	Agree to some extent	Disagree to some extent	Fully disagree	I don't know
The organization must strongly acknowledge the contents of the security area in future security development.	Fully agree	Agree to some extent	Disagree to some extent	Fully disagree	I don't know

Table 3: Phase 1 questionnaire statements

After the run-through of the definitions I asked the participants to submit the forms so they would be available for review. The group examined the answers per area and based on the division of opinions we aimed to find out the common view for the group. The following logic was applied in the analysis: does the majority agree, disagree or not know, do the marginal answers support the majority in terms of positive or negative alternatives, and does the group agree with the conclusion. Based on the common view, began the delimitation of prospect security areas for further processing. The number of areas that continue to the next phase was set to five. Discussion and the perceived importance of a security area guided the determining of the prospects. The design of the questionnaire statements and the assessment possibilities aimed to reveal where the possible focus and priority areas lie. The interest was in finding consistencies as well as inconsistencies from the common view. Also, it was considered to be valuable information if there seemed to be no knowledge of the state and/or importance of a security area.

As a result, the implementation phase successfully produced as planned the documented personal views of the security coordinators, documented common view of the security coordinators and the documented preferred scope of development, with initial connections to FRC's own environment. In accordance with the theoretical background, the workshop enabled the implementation of service design principles, where working should be human-centric and collaborative. In general, the workshop promoted common understanding of security areas by utilizing a national benchmark and raised the awareness of the comprehensiveness of security. It allowed to find out the general state of different security areas, but also the relevance and importance of the security areas in relation to FRC, based on views of the security coordinators. Furthermore, Phase 1 provided the needed linkage and

baseline to the next phase of the process. The tools, the translated (original documents are in Finnish) online questionnaire and the summary table templates, used in the process are available in the Appendix 1 and 2.

3.2 Phase 2: Identifying organizational priorities

The role of the second phase in the process was to build on the insight of the security coordinators and draw information from the internal operational organization. It applied the sequencing principle of service design to drive a comprehensive orchestration of security management and began to build the documented understanding of the security contexts and awareness within the organization, which were emphasized in the management system standards.

Implementation was conducted in a form of an online survey, using the same platform as the baseline questionnaire. A survey is a structured, quantitative, data collection method that usually has a person as the unit of observation, whose opinions, attitudes and characteristics are under research. (Finnish Social Science Data Archive 2021b.) As the intention was to find out the perceptions of security of a larger sample than a simple focus group, this method was a good fit for the implementation of this phase. Similar to the first phase, the survey aimed to find out the condition and importance of different organizational security areas. The sample group represented the FRC from all operational functions which gave a good overview on the organization. The survey was designed to gain complementary information in support of the security coordinator insight from the Phase 1. The process of design is depicted in the figure 4 below.

Figure 4: Survey design process

The design process began with the review of previous phase outputs and the reference material with the intention to produce short descriptions of chosen security areas that would have relevance to the organization in general. This was incremental, as the main difference between the survey and the workshop was that the respondents did not get any other explanation of the terminology and concepts of organizational security than what they will get in the survey. This had to be kept in mind also with the composition of the survey, so that

the information collected would be relevant and that the survey serves the purpose of increasing awareness of organizational security as well. An example of a possible definition for personnel security that links to an organization via threat scenarios is presented in table 4 below.

Personnel security	Personnel security aims to ensure the security and capability of people by protecting them from crimes (e.g. violent situations or threats towards customer service) and emergencies, which are not regularly present in the daily work (compare Occupational Health and Safety OHS). Additionally, it aims to secure the critical personnel resources in the organization as well as prevent and avert transgressions and criminal activity caused by the internal organization (e.g. frauds). Methodologies of personnel security might include for example different security guidelines, e.g. threat scenarios and travelling, back-up personnel arrangements of organizational key personnel, close protection, security clearances related to recruiting and non-disclosure agreements.

Table 4: Modified example definition, Personnel security
(Confederation of Finnish Industries n.d.)

Continuing the survey design process, a first draft was made that was further processed in cooperation with the FRC representative. With the consideration that the respondents would not get any other explanation than what is in the survey, the survey was therefore built of an orientational assessment part that discussed their resources and vulnerabilities to conduct normal work and a security assessment part that considered the organizational security areas. The security areas were given compiled definitions from CFI model using relevant threat examples according to the example framework in table 4 to illustrate the possible meaning of the areas to FRC. Both, the orientational and the security assessment parts, involved similar answering options from the Likert scale theory as used in the Phase 1 baseline questionnaire, which allowed consistency in analysis. An example excerpt of the orientational assessment of resource vulnerabilities is illustrated in table 5 below.

Resource vulnerability statement	**Assessment**				
Personnel; the critical tasks of the unit depend heavily on competence of individual people.	Fully agree	Agree to some extent	Disagree to some extent	Fully disagree	I don't know
Facilities; the critical tasks of the unit are dependent of the accessibility and availability of facilities.	Fully agree	Agree to some extent	Disagree to some extent	Fully disagree	I don't know

Table 5: Example excerpt of the orientational assessment part

The Likert scale assessments were complemented with an arrangement of priorities in the orientational part and open complementary questions in the security area part. The final composition of survey sections is presented in the table 6 along with a context reference to the survey structure. In addition to exposing the perceptions of current state and meaning of security, the survey itself aimed to reveal the possible "hot topics" or genuine insights that come to mind considering the security areas during the survey by allowing to type in comments after each evaluation. Also, the survey included the possibility to announce interest in further discussion about the security areas with the security coordinators of the FRC. The schedule for answering was set to one week, from the experiences of both the author and the FRC representative that the answering percentage of such surveys tend not to benefit from a much longer period. Also, as the main objective of the survey was to gather complementary information and begin to introduce security themes to the organization, the robustness of the survey did not have be too thorough. Meaning that it is usually recommended to apply multiple rounds of surveys to increase the number of responses (Finnish Social Science Data Archive 2021b). In this project the survey was decided to deploy only once to maintain the project schedule. However, to assist in the interest of taking the survey, the questionnaire was designed to be structured on the mandatory parts and open in voluntary sections. The average reply time was estimated to be between 5-15 minutes, making it a relatively quick task to accomplish. This is in line with the instruction of The Quantitative Methods Guidebook that a survey should not exceed 15 minutes in answering time (Finnish Social Science Data Archive 2021b). To provide more credibility, it was agreed that the client representative would forward the survey link to the internal organization. The translated version of the survey is available in its completeness in Appendix 3.

No.	Survey section	Design context
1.	Unit name	Demographics
2.	Resource vulnerabilities in the unit	Orientational assessment part
3.	Priority of resources in the unit	Orientational assessment part
4.	Current state and importance evaluation of a security area	Security assessment part
5.	Open comment for development ideas in the scope of the evaluated security area	Security assessment part
6.	Signal of interest for further discussion considering the evaluated security areas	Sample group engagement

Table 6: Survey composition

After the answering schedule had passed the results were exported into an Excel-file for closer examination. The data was analysed by starting from the security areas with the same logic as in Phase 1: does the majority agree, disagree or not know and do the marginal answers support the majority (positive or negative alternative). As there was no ability to reach a group consensus via discussion, the complete agreements and disagreements were used to emphasize the security areas. This information was then compared to the information considering resources and vulnerabilities from the orientational parts as well as to the resource priority orders, and still further compared to the security coordinator insights from Phase 1. From this analysis a group of three security focus areas began to emerge. These three areas were eventually chosen for further processing in phase 3 with the security coordinators.

The results of the survey appeared logical and consistent without deviation from the expected. It, however, showed in the answering activity that the survey was sent only once. But as mentioned previously, this phase intended to create complementary information and increase awareness and, in that sense, it successfully managed to produce the outputs of Documented and analyzed views of the organization on safety and security and Documented focus areas for organizational security development as described in the General Process Model. The method of Phase 2 continued logically in relation to Phase 1 as planned. It

continued to implement the CFI principle of layered approach and the added value principle to customer and internal process from service design by introducing the internal perspective of the organization. These in total contribute to the contexts understanding and scoping that are needed in developing organizational security management. Finally, using the same online format as the baseline questionnaire in the Phase 1 had many advantages, as it allowed to keep the project pragmatic and functional by controlling the amount different platforms used, while demonstrating the effectiveness of a simple platform in multiple use cases.

3.3 Phase 3: Focusing and deepening the insight

Phase 3 was designed to reveal concrete development targets that are based on validated organizational insight. Implementation included the final workshop of the project where the gathered situation picture was refined and deepened. The methodology based on a national framework for continuity management from the theoretical background, the KUJA model of the Association of Finnish Municipalities, and especially the KUJA speed test tool (Pikatesti). The checklist-type of tool aims to reveal whether an organization should consider development actions in relation to its current state of continuity management by reviewing items such roles, responsibilities, policies, guidelines, communication, risk management, and stakeholder and supply chain management (Association of Finnish Municipalities 2019b). It reflected well on the ISO based management system thinking and offered a logical and simple way to include the managerial perspective into the assessment process. The KUJA framework suited well to the purposes of this phase, as the aim was to create a better understanding of the current state of security management in the three security areas that the previous phases indicated as focus points. In addition, it matched the workshops aims, which seeked to provide a platform to further increase the awareness of the comprehensiveness of security, find out focus topics for future development, discuss other observations that might affect the current state of a security area and provide linkage and documentation for follow-up activities.

As the KUJA-model focused on management of continuity, the speed test tool did not apply as is. However, with a simple redesign, it provided a great benchmark and an adequate tool to assess security management in general. The redesign began by importing the KUJA speed test statements from their original Microsoft Word environment (Association of Finnish Municipalities 2019b.) into a Microsoft Excel sheet and modifying them to cover more comprehensively the security management domain, instead of continuity only. Building the tool in Excel allowed the assessment of all areas separately in the same template whilst building the same time an effective overview picture of the situation through colour-coding. Each security area was assigned a separate column and the statements to be assessed were added to rows. To complete the assessment, the question for each security area per statement was: is the statement X regarding the area Y considered to be OK (green colour),

Not OK (red colour), Incomplete (yellow colour) or Unknown (blue colour)? An example excerpt of the tool is portrayed in the figure 5 below and the complete translated tool can be found from the Appendix 4.

	Assessment date:	Assessment of security areas			
No.	Assessment question	*Security area 1*	*Security area 2*	*Security area 3*	Comments
1.	Area has been clearly defined and is applicable from the organization's perspective (i.e. scope).	OK	Partially OK	Not OK	
2.	Activities regarding the area are guided by a management approved policy along with complementing guidelines and/or development programs.	Unknown/Needs investigation			
3.	Roles and responsibilities regarding the area have been documented and defined. Related contact persons are up to date.				

Figure 5: Example excerpt of the assessment tool

In the workshop, similar to the Phase 1 workshop, the group composition was myself as the facilitator and the participants represented the personnel involved in organisational security. This time the workshop was eventually set to a two hour timeframe of which half an hour was reflective discussion with the group about the previous phases and the actual workshop was conducted within an hour and a half. The session still fitted into a timeframe of a rather normal stakeholder meeting, providing the pragmatic approach for the process in general. Process for the workshop was fairly simple after the introductionary discussion: Reflect on the previous phases and their output, assess the security areas with the assessment tool. The introductionary phase had an emphasized value in the process to tune the participants to a correct mode. The followed discussion about the previous phase results, the conclusions made of them and their relevance in regard of FRC was necessary to frame the appropriate setting for the assessment discussion. The keyword in this workshop was active dialogue. Nevertheless, it required a strong presence of the facilitator to avoid the discussion fall into too technical details or to stall under possible uncertain assessment statements. The assessment itself was based on the experience and intuition of the security coordinators as well as the flowing discussion during the workshop and the insights the emerged from the dialogue. These were complemented, where necessary, with the insight from the internal organization, based on phase 2 open comments, resource vulnerabilities and resource priorities.

In the scope of the development project, there was no further need for analysis after the assessment, as the workshop generated a clear mapping of the current state of security management characteristics that should be considered in future planning. As a result, Phase 3 successfully produced the planned General Process Model output: Documented security management current state of the focus areas. The fourth phase provides an assessment of validity on the methodologies used. General suggestions of possible following activities are given in the Conclusions -chapter.

3.4 Phase 4: Validating, concluding & reporting

This phase included the validation of data and the methods in different phases along with a compilation of previous elements into clear reports. Applying the layering principle and a variance in methodology ensured that the outputs connect to the organization's environment in a diverse enough way as is the nature of organizational security to begin with. Moreover, keeping in line with service design theories, a single method only would not even be able to offer enough added value. Sometimes many iterations and pivots are needed before finding the right fit (van der Pijl et al. 2016).

The United Nations Office on Drugs and Crime (UNODC) provided a method in the Criminal Intelligence Manual for Managers (2011), the 6x6 system, that is used in the intelligence communities to evaluate the data and source validity. It is explained that data evaluation is a critical part of gaining a justified understanding, or inference, of a subject. "The validity of an inference is directly linked to the quality of the data behind the inference" (UNODC 2011, 13). A disciplined analysis must consider all gathered information, as too early exclusion, for instance in the beginning of the process, could lead to a vital piece of information being overlooked which could lead to an incorrect analysis and jeopardize an enquiry. Emphasis on the premises of information as the root of an inference on the other hand should be reiterated with the logic "the premises that led me to my inference are…", instead of using information only to support an already made hypothesis. This ensures that the intelligence process arrives to a well-supported estimation or conclusion. According to UNODC, three fundamental principles apply to evaluation, where it must be based on professional judgement and not be influenced by personal feelings, the source must be evaluated separately to the information and the evaluation must be carried out as close to the source as possible. (UNODC 2011.) For the purpose of source relevant validation that would cover the used implementation methodologies as well, a service design validation canvas was a great fit. It was introduced by Patric van der Pijl, Justin Lokitz, Lisa Kay Solomon, Erik van der Pluijm, and Maarten van Lieshout in their book Design a Better Business: New Tools, Skills, and Mindset for Strategy and Innovation (2016). They explain that the goal of the validation process is to learn as much as possible, as fast as possible. The table 7 below introduces a modified version of their validation canvas which responds to the needs of this phase without compromising the essence of the validation process.

	Phase 1 methodology	Phase 2 methodology	Phase 3 methodology	Phase 4 methodology
Riskiest assumption	The designed tools create a significant amount of active dialogue within the group that provides deeper knowledge and numerous silent ques relevant to FRC about the state of security.	The survey indicates clear areas of focus that the majority of the internal organization promote along with insightful open commentary.	The assessment tool will provide a clear overview of the current state in security management and will be the backbone of all near future development activities.	Validation and compilation of results provide unique information not produced or recognized during the other implementation phases.
Target segment	Security coordinators	Internal Organization	Security coordinators	Project coordination / FRC representative
Minimal success criterion	All designed tools will be used as planned to document the necessary information for phase 2.	The survey gets answers and open commentaries from the optional sections.	The assessment tool can be used for an assessment and is considered helpful to decide future development.	The data and the methods can be considered valid and the compilation format provides the central information in an organized and logical manner.
Results	Phase 1 minimal success criterion was achieved along with some discussion that provided additional insight. The workshop timeframe would have to be increased to allow deeper discussion of security area relevancies to FRC in the initial phase.	Phase 2 minimal success criterion was achieved. Survey results pointed out clear priorities in resources and uncertainty considering security areas. The survey managed to engage respondents in the open and voluntary sections.	Phase 3 minimal success criterion was achieved. The tool provided a rather clear overview of different security management topics and their estimated current state, which can be reviewed on glance via a heatmap.	Phase 4 minimal success criterion was achieved.

Table 7: General Process Model validation
(van der Pijl, et al. 2016)

The UNODC method, the 6x6 system, provided an overall confirmation for the conclusions and built on the insight of the service design method. The 6x6 evaluation scales are presented below in the tables 8 and 9. The evaluation itself reflects the data collection in general during the development project. A full and proper evaluation, according to the manual, requires the assessment of the reliability of the source and the validity of information. (UNODC 2011). Overall, according to this method, the data can be considered valid as it has been built consistently on top of sequent findings and compared to the already existing information before moving on. The data has been built in co-operation with security coordinators and consistent with the findings from the organizational survey. Based on the assessment tables, the collected data in different implementation phases was deemed A1 grade, i.e. confirmed and completely reliable.

Grade	Definition
A Completely reliable	▪ No doubt regarding authenticity, trustworthiness, integrity, competence. ▪ History of complete reliability.
B Usually reliable	▪ Some doubt regarding authenticity or trustworthiness or integrity or competence (one count). ▪ History of general reliability.
C Fairly reliable	▪ Doubt regarding authenticity, trustworthiness, integrity, competence (two counts and more). ▪ History of periodic reliability.
D Usually not reliable	▪ Definite doubt regarding authenticity, trustworthiness, integrity, competence. ▪ History of occasional reliability.
E Unreliable	▪ Certainty about lack of authenticity, trustworthiness, integrity, competence. ▪ History of unreliability.
F	▪ Cannot be judged.

Table 8: Source reliability evaluation
(UNODC 2011)

Grade	Definition
1 Confirmed	▪ Confirmed by other independent sources. ▪ Logical in itself. ▪ Agrees with other information on the subject.
2 Probably true	▪ Not confirmed independently. ▪ Logical in itself. ▪ Agrees with other information on the subject.
3 Possibly true	▪ Not confirmed. ▪ Logical in itself. ▪ Agrees somewhat with other information on the subject.
4 Doubtfully true	▪ Not confirmed. ▪ Not illogical. ▪ Not believed at time of receipt although possible.
5 Improbable	▪ Confirmation available of the contrary. ▪ Illogical in itself. ▪ Contradicted by other information on the subject.
6	▪ Cannot be judged.

Table 9: Data validity evaluation
(UNODC 2011)

During the final stages of project FRC received the detailed data and other material as well as a presentation that highlighted the central findings and provided development suggestions. This finalized thesis report was another deliverable of Phase 4. As a result, the validation indicated that the designed General Process Model functioned as planned and it proceeded in a logical and justifiable manner. The phase successfully produced the intended outputs of Documented validation of data and methods as well as the Compiling project reports with follow-up suggestions. Chapter 4 continues with the overall evaluation of the development project itself and offers further remarks on the created assessment model. Finally Chapter 5 concludes the report with ideas on how to proceed after the assessment process.

4 Project evaluation

This project gave a fairly clear image of how security is perceived within the operational personnel of an organization. Especially in situation where resources to actually implement development initiatives or even drive them into a pipeline were scarce, the approach of "understanding the client" had much to its advantage. The Client got tools to communicate and "market the worth" of security and build common awareness, but also insight to direct those scarce resources to meaningful activities that, when successfully completed, should increase the buying power of security initiatives even more.

In contrast to creating situational awareness on purely technical elements of security, this project should have offered a refreshing take on how to view security as a "marketable internal service," if you will. The whole intelligence gathering process aimed to find about those elements that define whether or not the technical implementations of security are bound to be successful in the future. "Those elements" refer to the end-users that are expected to follow through the guidelines and adopt possible new habits and ways of working. This kind of approach proposes inclusion, proactivity and communication to be incremental values for managing security and its development – hopefully, eventually, increasing the meaning and value of different initiatives in the eyes of the personnel.

4.1 Time management

The project schedule was planned to spread over 21 weeks, adding two weeks as a hazard marginal. This considered the planning of the project and presentations of the results. Eventually the project stayed right on the schedule.

The project implementation had been designed with sufficient enough marginals to complete the project in time, while allowing possible schedule changes or even delays. However, some observations already during the scoping period of the project accurately indicated, that there would be a need to practice quite vigilant time management and active communication with the client to mitigate possible risk of conflicts considering scheduling priorities for the necessary meetings in relation to the thesis. Having made this observation in advance and being able to respond to the challenge was probably one of the central elements in keeping the project on time.

Key take-aways from the time management in this project.

1. long planning period,
    a. reflects to a large amount of scoping done in order to produce timely and quality results. This was also an incremental factor for the success of the implementation.

2. Discussions and open communication channel with the Client representative
    a. continuous dialogue during the project timeline, in order to maintain a good overview of the state of implementation.

4.2 Ethics and risk management

The development project report was produced and published as an academic report. While the project was functional and not theoretical research, the principles of The Finnish Advisory Board on Research Integrity guidelines for Responsible conduct of research and procedures for handling allegations of misconduct in Finland (2012) were still applicable and were complied with, where necessary.

Following the appointed Ethical recommendations for thesis writing at universities of applied sciences by The Rectors' Conference of Finnish Universities of Applied Sciences Arene (2020), the project implementation and reporting had a written agreement and the publicity of results and the thesis had been discussed in advance.

The project had no monetary budget nor compensation, the currency used was time and labor which were not comprehensively documented. Exchange of personal and confidential information happened only where necessary, and instances were reviewed by each case. Data collection was designed so that there was a nearly non-existent risk of exposing too sensitive material.

4.3 Collaboration and communication

Co-operation with the Finnish Red Cross succeeded well in this project, much due to the careful planning stage and proper anticipation of scheduling priorities. Also, the proactive approach of FRC in sense of gaining access to relevant documentation for example were key factors to the completion of the project.

A rather active communication regime ensured that all parties were up to date. This project served the interests of both the FRC and the author making the frequent connections a mutual benefit. The planning stages and larger issues, such as how the internal organization survey will look like and be structured were addressed in online meetings that were usually booked to an hour-long time slot. Minor issues and other informing happened via phone, either calling or in most cases via instant messaging.

4.4 Assessment model (General evaluation)

The assessment model can be considered successful from the overall perspective. It answered to the original needs of the FRC about gaining oversight of the current state of security. The question in general level was how to assess the organizational security so that it brings

awareness to the organization involved. The assessment should expand the toolbox for security development, consider how the organization could be connected in the assessment process and ensure that the assessment could be reproduced in the future. All of these elements were incorporated into the general process and achieved through implementation. Also, as reported in the implementation phase descriptions, all planned outputs were produced within the scope of this development project. The scope of the assessment was eventually focused to the management level of security, which in the future will provide more support in developing more technical and specific elements of security. The implementation outputs of different phases should be taken to an active review in short-term future after completing the general process model and plan the following steps. The process itself is fairly straightforward to allow repeatability when accompanied with the guidelines of this report and using the free tools this project produced. The tools are described in the Appendices, but to gain full mobility and functionality for another use case, similar to the methodology described in this report, they must be replicated and created again to their original environments. For example, the questionnaires need to be created to an online form and the assessment tool to an Excel spreadsheet.

5 Conclusions

Organizational security is a complex and interesting domain that requires a lot of contexts understanding. Key observation already in the early stages of the project was that if the project is intended to have any applicability value during and after the project, the scope must be defined very clearly and the scope has to connect to the current needs of the organization. Second key was to understand the role of the end-users in order to build sustainable paths of development that can be relevantly communicated to the organization and other interested parties.

The methodologies in **Phases 1 and 2**, provide critical information to build necessary situation awareness on organizational security. Accurate situation picture allows better future decisions and justification of resource acquisitions regarding security development. In these future ventures, the organizational security personnel of FRC will become the service providers in relation to the internal organization and other interested parties. Phases 1 and 2 offer a sustainable way to integrate customer-centricity and collaboration to the FRC in the spirit of service design theories, by reviewing the perceptions of current state and the desired priorities of the internal organization and security coordinators. **Phase 3** directs the practitioner of the methodology to consider the basic composition of organizational management from the security perspective. The foundational idea that must be understood is the importance of defining terms and concepts, deriving executive management approved policies and guidelines from those concepts along with allocating clear roles and

responsibilities. Their primary purpose is to ensure common understanding and enable an effective communication, but also to maintain the necessary documentation that are critical in responding to threat events and recovering from crisis situations, for instance. In all of the phases, but especially when deepening the insight, it is important to remember that the evaluation options provide the possibility to also answer "I don't know or Needs clearance." This should be considered as valuable information as the others because it opens helpful follow-up questions such as why there is no knowledge of this topic, should we know about this topic, when we need to have an understanding of this topic and what it requires to attain this understanding? **Phase 4** reminds the value of evaluating the validity of the process itself and the data used in it. If decisions of actions are based on assumptions of only few persons with a limited linkage to the organization's operational environment, it can lead to a situation where resources and focus are directed to completely irrelevant domains. This is not an entirely unreversible position, but it has a great potential to crumble the credibility of organizational security function and weaken the future possibilities of development.

When making plans for development initiatives after the assessment process, an organization should consider that each security area has individually already a lot of depth, especially when introducing the more technical layers. Therefore, it might be wise to begin development with one area of security only and then copy that process to other areas of security. It should be noted that the security areas overlap on many occasions and with the solutions and controls of one area, an organization can affect to the threats rising from another area. A thorough risk management practice helps to identify these scenarios. Usage of existing benchmarks is highly recommended as there are several publicly available and they usually are products of continuous long-term iteration and respond well to different organizational needs. The managerial efforts of establishing clear roles, responsibilities, action patterns and communication channels already alone can take the organization a huge leap forward as they force the organization to involve a lot of discussion on how different scenarios should be handled and with what resources. The positive note is also that they do not require large investments but can be budgeted into working hours. This, however, does not make the managerial approach any less difficult as security themes might still generally be understood as costs rather than services that provide added value for operations. With this assessment model the organization, and specifically the security function, can begin to communicate the value aspect as well and introduce the security concept as a natural part of organizational management practices, as it should be.

References

Electronic

Barros, O. 2017. Business Engineering and Service Design, Second Edition Volume I. Business Expert Press. Accessed 13 November 2021. ProQuest Ebook Central. https://ebookcentral.proquest.com/lib/laurea/detail.action?docID=4717717

Brooks, D. 2010. What is security: Definition through knowledge categorization. Security Journal 23:225-239. Accessed 20 October 2021. ResearchGate. https://www.researchgate.net/publication/247478178_What_is_security_Definition_through_knowledge_categorization

Casino, F., Dasaklis, T. & Patsakis, C. 2019. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics Volume 36. Accessed 20 October 2021. https://www.sciencedirect.com/science/article/pii/S0736585318306324

Finland. 2017. Presidential Decree on the Finnish Red Cross 1.12.2017/827. Accessed 15 September 2021. https://www.finlex.fi/fi/laki/alkup/2017/20170827

Finnish Red Cross. 2020. Rednet: Sääntökirja. Accessed 15 September 2021. https://rednet.punainenristi.fi/system/files/page/spr_saantokirja_2020_100x150_FIN_LR%20%281%29.pdf

Finnish Red Cross. 2021a. RedNet: Vuosikertomus 2020. Accessed 15 September 2021. https://rednet.punainenristi.fi/system/files/page/SPR_Vuosikertomus_2020_FIN_low.pdf

Finnish Red Cross. 2021b. RedNet: Fact Sheet about Finnish Red Cross. Accessed 15 September 2021. https://rednet.punainenristi.fi/system/files/page/Fact-Sheet_SPR_p%C3%A4ivitetty07062021.pdf

Finnish Social Science Data Archive. 2021a. Laadullisen tutkimuksen verkkokäsikirja. Accessed 20 September 2021. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/

Finnish Social Science Data Archive. 2021b. Kvantitatiivisen tutkimuksen verkkokäsikirja. Accessed 20 September 2021. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvanti/

Finnish Standards Association. 2021. SFS-EN ISO 22300:2021:en Security and Resilience Vocabulary (ISO 22300:2021). SFS 2021-03. Accessed 20 October 2021. https://online.sfs.fi/fi/index.html.stx

Flood, R. 1999. Rethinking the Fifth Discipline: Learning Within the Unknowable. Taylor & Francis Group. Accessed 20 November 2021. ProQuest Ebook Central. http://ebookcentral.proquest.com/lib/laurea/detail.action?docID=165413

International Organization for Standardization. 2019. ISO 22301:2019(en) Security and resilience — Business continuity management systems — Requirements. Accessed 20 October 2021. https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en

Jacobs, G., Suojanen, I., Horton, KE. & Bayerl, PS (eds). 2020. International Security Management: New Solutions to Complexity. Springer International Publishing AG. Accessed 10 November 2021. ProQuest Ebook Central. https://ebookcentral.proquest.com/lib/laurea/reader.action?docID=6287858

Lanne, M. 2007. Yhteistyö yritysturvallisuuden hallinnassa - Tutkimus sisäisen yhteistyön tarpeesta ja roolista suurten organisaatioiden turvallisuustoiminnassa. VTT Publications 632. Accessed 30 October 2021.
https://www.vttresearch.com/sites/default/files/pdf/publications/2007/P632.pdf

Morelli, N., de Götzen, A. & Simeone, L. 2021. Service Design Capabilities. Springer International Publishing. Accessed 13 November 2021.
https://link.springer.com/content/pdf/10.1007%2F978-3-030-56282-3.pdf

National Security Authority, Finland. 2020. KATAKRI 2020 - National Security Auditing Criterion. Accessed 30 October 2021. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Nieminen, M., Talja, H., Heikkilä, JP., Airola, M., Viitanen, K. & Tuovinen, J. 2017. Muutosjoustavuus – Organisaation resilienssin tukeminen. VTT Technology 318. Accessed 30 October 2021.
https://www.vttresearch.com/sites/default/files/pdf/technology/2017/T318.pdf

Prime Minister´s Office, Finland. 2017. Kolmas sektori viranomaisten turvallisuustoiminnan tukena. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 76/2017. Accessed 20 September 2021.
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160404/76_Loppuraportti%20kolmas%20sektori%20viranomaisten%20turvallisuustoiminnan%20tukena_editoitu%205122017.pdf

Sennewald, C. 2011. Effective Security Management. Elsevier Science & Technology. Accessed 2 November 2021. ProQuest Ebook Central.
http://ebookcentral.proquest.com/lib/laurea/detail.action?docID=680862

Stenberg, I. 2017. Turvallisuuskulttuuri Maanpuolustuskorkeakoululla. Yleisesikuntaupseerikurssin diplomityö. Yleisesikuntaupseerikurssi 58 Merisotalinja. Accessed 15 October 2021.
https://www.doria.fi/bitstream/handle/10024/144314/Stenberg%20IST_diplomity%c3%b6_YEK58.pdf?sequence=1&isAllowed=y

Stickdorn, M., Hormess, M., Lawrence, A & Schneider, J. 2018. This Is Service Design Doing: Applying Service Design Thinking in the Real World. O'Reilly Media, Incorporated. Accessed 20 September 2021. ProQuest Ebook Central,
http://ebookcentral.proquest.com/lib/laurea/detail.action?docID=5219777

The Finnish Advisory Board on Research Integrity. 2012. Responsible conduct of research and procedures for handling allegations of misconduct in Finland. Guidelines of the Finnish Advisory Board on Research Integrity 2012. Accessed 15 September 2021.
https://tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf

The Finnish Terminology Centre. 2017. TSK 50 Vocabulary of Comprehensive Security. Accessed 20 October 2021.
http://www.tsk.fi/tiedostot/pdf/Kokonaisturvallisuuden_sanasto_2.pdf

The Finnish Terminology Centre. 2018. TSK 52 Vocabulary of Cyber Security. Accessed 20 October 2021. http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

The Rectors' Conference of Finnish Universities of Applied Sciences Arene. 2020. Ethical recommendations for thesis writing at universities of applied sciences. Accessed 15 September 2021. https://www.arene.fi/wp-content/uploads/Raportit/2020/ETHICAL%20RECOMMENDATIONS%20FOR%20THESIS%20WRITING%20AT%20UNIVERSITIES%20OF%20APPLIED%20SCIENCES_2020.pdf?_t=1578480382

Uchendu, B., Nurse, J., Bada, M. & Furnell, S. 2021. Developing a cyber security culture: Current practices and future needs. Computers & Security Volume 109. Accessed 20 October 2021. https://www.sciencedirect.com/science/article/pii/S016740482100211X

United Nations Office on Drugs and Crime UNODC. 2011. Criminal Intelligence - Manual for Managers. United Nations Office at Vienna. Publishing and Library Section. Accessed 9 November 2021. https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Managers.pdf

van der Pijl, P., Lokitz, J., Solomon, L., van der Pluijm, E. & van Lieshout, M. 2016. Design a Better Business: New Tools, Skills, and Mindset for Strategy and Innovation. John Wiley & Sons Incorporated. Accessed 30 October 2021. ProQuest Ebook Central. https://ebookcentral.proquest.com/lib/laurea/detail.action?docID=4694619

Wang, B., Wu, C., Kang, L., Reniers, G. & Huang, L. 2018. Work safety in China's Thirteenth Five-Year plan period (2016–2020): Current status, new challenges and future tasks. Safety Science Volume 104. Accessed 20 October 2021. https://www.sciencedirect.com/science/article/pii/S0925753517318593

Unpublished

Association of Finnish Municipalities. 2019a. KUJA Arviointityökalu. Accessed 15 October 2021. https://www.kuntaliitto.fi/yhdyskunnat-ja-ymparisto/turvallisuus-ja-varautuminen

Association of Finnish Municipalities. 2019b. KUJA Pikatesti. Accessed 15 October 2021. https://www.kuntaliitto.fi/yhdyskunnat-ja-ymparisto/turvallisuus-ja-varautuminen

Association of Finnish Municipalities. No date. Website: Yhdyskunnat ja ympäristö – Turvallisuus ja varautuminen. Accessed 15 October 2021. https://www.kuntaliitto.fi/yhdyskunnat-ja-ymparisto/turvallisuus-ja-varautuminen

Cambridge University Press. No date. Cambridge Dictionary: Organization. Accessed 30 October 2021. https://dictionary.cambridge.org/dictionary/english/organization

Confederation of Finnish Industries. No date. Yritysturvallisuus. Accessed 20 September 2021. https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/

Digital and Population Data Services Agency. 2021. Suomidigi website: VAHTI-ohjeet. Accessed 30 October 2021. https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet

Figures

Tables

Appendices

Appendix 1: Baseline questionnaire, Phase 1

Organizational security workshop

Hi,

the workshop uses the organizational security model by Confederation of Finnish Industries (CFI) as a framework. From this frame, we will specifically use the division of different areas in security and their definitions (link below, the definitions, in Finnish, can be found by scrolling down and opening the information boxes on each security area from the plus-symbol).

In the first part of the workshop we will go over the model using this baseline-questionnaire as a tool.

Guidance on filling the questionnaire:

1. Familiarize yourself with the CFI definition of a security area. Link below:
   a. https://ek.fi/hyotytietoa-yrityksille/yritysturvallisuus/ (https://ek.fi/hyotytietoa-yrityksille/yritysturvallisuus/)
2. Using the definition, assess from the organization's **applicable** perspective each area's:
   a. Current state
   b. Importance for the organization in security development

* Pakollinen

1. The area of [*security area name*] *

	Fully agree	Agree to some extent	Disagree to some extent	Disagree fully	I don't know
Considering the nature of the operation, the organization covers the contents of the security area at least sufficiently.	◯	◯	◯	◯	◯
The organization must strongly acknowledge the contents of the security area in future security development.	◯	◯	◯	◯	◯

Appendix 2: Summary table templates, Phase 1

Common view

Security area	1) Considering the nature of the operation, the organization covers the contents of the security area at least sufficiently	2) The organization must strongly acknowledge the contents of the security area in future security development
Personnel security		
Property and premises security		
Rescue safety		
Production and operational security		
Environmental security		
Information security (including cyber security)		
Transgression and incident management		
Preparedness and crisis management		
Occupational health and safety (OHS)		

Focusing

- Five security areas of which we want to get the organization's perspective.
- What threats could rise from these areas that could affect the organization and its operations?

Prioritized security areas	Threats to the organization
[Security area 1]	
[Security area 2]	
[Security area 3]	
[Security area 4]	
[Security area 5]	

Appendix 3: Online survey, Phase 2

Organizational security survey

Hi,

this survey maps the current state of areas related to organizational security and their importance in future development work. The areas and their definitions stem from the organizational security model by Confederation of Finnish Industries (CFI). The security areas interested in this survey rise from the pre-assessment of the organization's security subject matter experts.

Guidance on filling the survey:

1. From the perspective of your operational unit, assess the vulnerability and priority of the central resources.
2. From the **applicable** perspective of your unit, assess each security area's
   a. Current state in the organization
   b. Importance for the organization in security development

The survey will take approximately 5-15min to answer.

NOTE! Do not fill personal information to the form!

* Pakollinen

1. Unit name *

2. Assess the vulnerability of your unit's resources *

	Fully agree	Agree to some extent	Disagree to some extent	Fully disagree	I don't know
Personnel; the critical tasks of the unit depend heavily on competence of individual people.	○	○	○	○	○
Facilities; the critical tasks of the unit are dependent of the accessibility and availability of facilities.	○	○	○	○	○
ICT-Technology (information systems, network, communication channels); the critical tasks of the unit are dependent of the functionality of information systems and networks.	○	○	○	○	○
Information; the critical tasks of the unit are dependent of the availability, integrity, usability and confidentiality of information (e.g. personal, customer or financial information, or area specific news etc.)	○	○	○	○	○
Internal and/or external supplier or partner etc.; the critical tasks of the unit are dependent of certain stakeholders such as subcontractors or vendors.	○	○	○	○	○

3. Considering your unit's operations, organize the previously assessed resources to an order of priority *

Personnel

Facilities

ICT-technologies

Information

Stakeholders

4. The area of [*security area name*] *

Example definition Personnel Security:
Personnel security aims to ensure the security and capability of people by protecting them from crimes (e.g. violent situations or threats towards customer service) and emergencies, which are not regularly present in the daily work (compare Occupational Health and Safety OHS)

Additionally, it aims to secure the critical personnel resources in the organization as well as prevent and avert transgressions and criminal activity caused by the internal organization (e.g. frauds).

Methodologies of personnel security might include for example different security guidelines, e.g. threat scenarios and travelling, back-up personnel arrangements of organizational key personnel, close protection, security clearances related to recruiting and non-disclosure agreements.

	Fully agree	Agree to some extent	Disagree to some extent	Disagree fully	I don't know
I am satisfied with the current state of the area in the organization.	○	○	○	○	○
The organization must strongly acknowledge the contents of the security area in future security development.	○	○	○	○	○

5. [*Security area name*] (optional)

What the organization should or must improve on this area?

6. I would like to discuss more about these areas with the security subject matter experts (optional)

E.g. observations, situation in the unit.

- ☐ [*Security area 1*]
- ☐ [*Security area 2*]
- ☐ [*Security area 3*]
- ☐ [*Security area 4*]
- ☐ [*Security area 5*]

Appendix 4: Assessment tool, Phase 3

	Assessment date:	Assessment of security areas			
No.	Assessment question	*Security area 1*	*Security area 2*	*Security area 3*	Comments
1.	Area has been clearly defined and is applicable from the organization's perspective (i.e. scope).	**OK**	**Partially OK**	**Not OK**	
2.	Activities regarding the area are guided by a management approved policy along with complementing guidelines and/or development programs.	**Unknown/Needs investigation**			
3.	Roles and responsibilities regarding the area have been documented and defined. Related contact persons are up to date.				
4.	Requirements of legislation and other regulation regarding the area have been identified and implemented as a part of operations and documentation.				
5.	There are up to date action plans/action cards regarding the area.				
6.	There are enough resources for management and development of the area.				
7.	Current state/status of the area is part of regular reporting regarding organizational security.				
8.	The area has been introduced to the personnel and necessary guidance and action plans are accessible.				
9.	Critical internal stakeholders and their roles and responsibilities have been documented and defined. Related contact persons are up to date.				
10.	Critical external stakeholders and their roles and responsibilities have been documented and defined. Related contact persons are up to date.				
11.	Area is recognized as a part of security risk management. Risks have been identified, assessed and processed accordingly and the management is documented. The progression of risks regularly followed and addressed.				
12.	Themes of the area are communicated, educated and practiced regularly in the organization.				