LAUREA AMMATTIKORKEAKOULU Uuden edellä

Development of a Structured Security Documentation Framework

Kinnari, Johanna

2013 Laurea Leppävaara

Laurea University of Applied Sciences
Laurea Leppävaara

Development of a Structured Security Documentation Framework

Johanna Kinnari
Master's Degree Programme in Security Management
Master's Thesis
May, 2013

Laurea-ammattikorkeakoulu Tiivistelmä
Laurea Leppävaara
Turvallisuusosaamisen ylempi ammattikorkeakoulututkinto

Johanna Kinnari

Turvallisuusdokumentaation rakenteen kehittäminen

Vuosi 2013 Sivumäärä 85

Tämän tutkimuksen tavoitteena oli kehittää ehdotus dokumenttirakenteeksi, jonka avulla on mahdollista luoda hallittavissa oleva turvallisuusdokumentaatiokokonaisuus. Rakenne kehitettiin ensisijaisesti Itella konsernin tarpeisiin. Itella on yksi Suomen suurimmista yritystyönantajista, joka tarjoaa palveluja tieto- ja tuotevirtojen digitaaliseen ja fyysiseen käsittelyyn. Palvelut tuotetaan Itellan kolmen eri toimialan toimesta kansainvälisesti.

Organisaation hallintotapakulttuuri ja tavoitteet määritellään hyvien politiikkojen kautta. Toimiva ohjausdokumentaatio muodostaa määritellyn rakenteen organisaation eri asiakirjoja varten. Mahdollisuus löytää punainen lanka dokumentaatiohierarkian alemmista dokumenteista aina siihen liittyvään politiikkaan ja perustana oleviin liiketoimintatavoitteisiin saakka kasvattaa ymmärrystä organisaation turvallisuustavoitteista, ja syistä turvallisuuteen liittyville hallintotavoille.

Jo tutkimuksen alkuvaiheessa alkoi näyttää siltä, että tätä aihealuetta ei ole tutkittu aikaisemmin. Kirjallisuutta tai tieteellisiä tutkimuksia, jotka kattavat tämän näkökulman perusteellisemmin ei voitu löytää. Aihealuetta ohuesti käsittelevä kirjallisuus kertoi pääosin liiketoiminnan ja turvallisuuden hallinnointitavoista, sekä ohjeisti turvallisuuspolitiikkojen sisällön kirjoittamiseen eri aiheista.

Koska kirjallista materiaalia nimenomaan dokumenttirakenteesta ei ollut saatavilla, käännyin ongelmani osalta eri organisaatioissa toimivien suomalaisten johtavien turvallisuusammattilaisten puoleen. Tein kyselytutkimuksen, joka paljasti lukuisia tapoja koostaa tämä turvallisuusdokumentointiin liittyvä rakenne ja rakenteeseen liittyvä hallinnointi.

Muodostin kyselytutkimuksen sekä kirjallisuusselvityksen pohjalta saatujen ideoiden ja ajatusten perusteella ehdotuksen turvallisuusdokumentaatiorakenteelle sekä sen nimeämiselle. Ehdotusta testattiin sekä asiantuntija-arviotimenetelmällä valittujen turvallisuusammattilaisten kanssa että kokeilemalla struktuurin käyttöä pöytätestaamalla tiettyjen tapausesimerkkien kautta. Pöytätestit toteutettiin Itellan sisäisesti.

Muodostettu rakenteellinen kehys soveltuu Itellan tarpeisiin, mutta asiakokonaisuuden ollessa yleinen, se varmasti soveltuu myös muiden organisaatioiden käyttöön. Koska Itellalla ei ole yleistä dokumenttirakennetta käytössä, ehdostusta turvallisuudendokumentaatiorakenteesta tullaan ehdottamaan myös Itellan yleiseksi dokumentaatiorakenteeksi.

Asiasanat (rivillä 54): turvallisuuspolitiikka, dokumenttirakenne, viitekehys, dokumenttiarkkitehtuuri

Laurea University of Applied Sciences
Laurea Leppävaara
Master's Degree Programme in Security Management

Abstract

Johanna Kinnari

Development of a Structured Security Documentation Framework

Year 2013 Pages 85

The objective of this thesis was to develop a proposal for a documentation framework which supports the creation of a manageable security policy framework. The framework was developed primarily for Itella Group. The Itella Group is one of Finland's largest employers, and it offers a wide-ranging set of information and logistics services in its three different business areas internationally.

The organization's governance culture and objectives can be defined by having good policies. A well-working policy framework will form a defined structure for different documents in an organization. The ability to trace lower-level documents to the original policy and to the business objectives gives understanding of the organization's security goals and reasons for security governance.

Already in the early stages of the study it appeared that this area has not been researched before as no literature or scholarly studies covering this angle more thoroughly could be found. The literature relating to this area was about business and security governance and about writing content of security policies concerning various subjects.

Hence, with the problem of finding written material, leading security professionals in several Finnish organizations were contacted. A survey was conducted, and the result of it revealed a plethora of ways to solve the common issue of security documentation structure and management of that structure.

Based on the questionnaire and ideas from the literature, a suggestion for a security documentation structure and its naming was built. This suggestion was tested both with an expert evaluation method with chosen security professionals and also by running case specific tabletop tests on the structure within Itella.

The framework will be suitable for the needs of Itella, but as the issue is general, this would also work for other organizations. Since Itella do not have an official common documentation structure in place, the security framework proposal is going to be proposed to be transformed also to the common documentation structure for the organization.

Key words (row 54): security policy, policy framework, document hierarchy, security architecture

Table of Contents

Acronyms used in this thesis

GENERAL

AEO	Authorised Economic Operator
CAB	Change Advisory Board
CISO	Chief Information Security Officer
EB	Executive Board
ISO	International Organization for Standardization
ISO/IEC 27001	Information security management system (ISMS) standard, version 2005
ISO/IEC 27002	Code of practice for information security management, version 2005
KATAKRI	Kansallinen turvallisuusauditointikriteeristö National Security Auditing Criteria (Finland)
MB	Management Board
NIST	National Institute of Standards and Technology
RFC	Recommendation/Request for Change
SABSA	Sherwood Applied Business Security Architecture
SOP	Standard Operating Procedure
TAPA	Transported Asset Protection Association
TOGAF	The Open Group Architecture Framework
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä Government Information Security Management Board (Finland)

ITELLA SPECIFIC

BG	Business Group
ISVT	Information Security Virtual Team
IT EB	Information Technology Executive Board

Acknowledgements

I would like to thank Itella Plc. and my employer Itella Information Inc. for the given opportunity and support for doing this thesis.

I offer my sincerest appreciation to my supervisor, Security Director Petri Puhakainen at the Tax Administration for his support and guidance for this project. I would also like to offer my deepest gratitude for Chief Information Security Officer Kimmo Helaskoski at Itella Plc.; it would not have been possible to write this thesis without the help and support from him. I would also like to thank Kimmo regarding many discussions we had when choosing the topic and when I was doing research and the writing process.

A special thanks to all the security professionals who were so kind to answer to my questionnaire. I am extremely grateful to the security professionals who also offered to be interviewed and especially to those four professionals who I chose to actually interview.

Finally, I thank my husband Teemu who has been my pillar in life and giving his never ending support. I also like to thank our families and friends for their positive encouragement.

Sincerely Yours,

Johanna Kinnari
Vantaa, Finland
May, 2013

1 Introduction

Corporate governance is a common practice in most of the organizations. Security, on the other hand, is a fairly new area of governance for many organizations even though it would be partly implemented. As Allen (2007, ix-xi) says "governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization's management does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, achieved, or sustained." The leaders of the governance level have authority, accountability, and resources to act and enforce compliance which other organizational functions do not have. (Allen 2007, ix-xi).

Currently the writer of this thesis does not know any other rational approaches which would help to achieve effective enterprise-wide security than implementing a security architecture containing its governance. Enterprises need ways to ensure their assets are adequately protected and available to use. A security governance program that includes a security policy management framework will assist in this task.

There has been a great amount of books, documentation, templates and discussion about policies and their development. There is still a lot of confusion about what the policies actually are. The guidelines are often limited to the policies themselves, how they should be written, and what they should contain. The discussion does not cover the documentation framework and structure behind it. It is unclear how well organizations structurize their policies and other related documentation. Who can issue a policy, which kind of entity can approve it and how to treat other policy supporting documents? Which kind of policy supporting documentation may or should exist?

Brotby (2009, 111) underlines that "it is common to see no distinction made between policies, standards, procedures, and guidelines, and they are often intermingled in an awkward amalgam". In a well-defined and built policy architecture, all business requirements can be traced downwards to security implementations. Likewise, any implementation or setting found has to be able to be justified by a business requirement. A policy framework should support this kind of refinement of rules for different levels of documentation. An important criterion for a successful framework is also maintainability. A well-structured system will support management of the documents by limiting content and redundancy between different documents.

Examples of a commonly used policy framework do not exist, and there is not a general understanding of what kind of structure a policy framework should have. Although this dilemma

is interesting, research around policy hierarchy is virtually non-existent. There is only one paper written by Baskerville and Siponen from 2002 which relates to the subject.

The need for a structured set of documents governing security and its implementations has grown from a practical need. In an enterprise like Itella, there exists a variety of documents guiding work and rules defining different issues. Problems arise when these documents cannot be put into any particular order, and the scope of them is not clear. This makes it difficult to figure out, which directives are in effect in different functions and tasks, which directives are recommendations and which are mandatory, and how to handle a contradictory ruling. The naming of documents does not help since many of them are called policies, even though their content might be varying from very general principles to the very small detailed instructions.

Also, the issuing and approval of documents is difficult when there is no clear structure. Detailed operational documents are brought for approval to board tables where only strategic and tactical issues should be in discussion.

The research in this thesis focuses on the policy hierarchy framework and forming a clear framework structure proposal for Itella Group (which will in this thesis be refereed as Itella). This work has been conducted with support from the Itella Corporate Security function. The used research methods have been Constructive Research together with Action Research. Research observations will be used to construct the structure for the proposal for a structured security policy framework for Itella. Framework will be evaluated via Expert Review method and tested in sessions within Itella.

1.1 Goal and objectives

The goal of this thesis is to develop a security policy management framework suitable for, at least, an Itella type enterprise's needs. It should be a clear and logical set containing a structure that makes it easier to find current directives and rulings which are applicable in different situations. This puts strength on the naming of documents but also having a reasonable control with a number of different kinds of levels of documents.

A successful outcome will contain at least the following:

- The document structure supports traceability of the solutions and decisions and chosen ways of implementation (top-down),
- The document structure supports justification of the solutions and decisions in the guiding of higher level documents (bottom-up),
- The document naming structure supports the document structure.

I will also use the term security policy architecture as well as security policy framework about this same construction. The security policy management framework contains a set of documents that make up how the enterprise protects its assets (people, information and infrastructure).

A comprehensive policy architecture is an effective management tool. Creation of that requires a security policy management framework to exist. The selected or formed security policy management framework should also enforce and allow the top-down traceability of solutions and decisions, as well as chosen ways of implementation. Along with traceability, it is important to find a justification for solutions and decisions in the higher level documents.

A policy framework provides a logical structure for organizing policies and additional documentation that supports the policies' implementation and enforcement. Security documentation is the means to translate the desired behavior into practical directives. It also provides guidance for individuals in the organization functioning in different organizational levels as well as forms the behavior of processes and functions when implemented.

In my duty as the leading Information Security Manager in one of Itella's Business Groups, I need to be able to define the required level of behavior and controls to secure our business within the Business Group. One of the requirements is to be able to be compliant with different requirements and also have evidence of that compliance. I think that the more transparent and simple the entire documentation framework is, the easier it would be for individuals to find the guiding and ruling documents that are relevant for them in their role.

Even the implementation of new regulations might be easier if the whole structure of requirements for security issues was more transparent. This will, for instance, lower the resistance of change since the need and the reasoning behind a certain rule is not a concoction created by "an evil security manager", but really a need the management has dictated.

This structure will be presented to Itella's Corporate Security and taken into use as soon as it is finalized and tested successfully for existing documentation.

1.2 Restrictions and exclusions

Developing the complete security policy architecture containing all the policies needed together with their content or guidance for content is beyond the scope of this thesis. I am not covering the content of the various document types in a detailed level. Instead, I am planning and developing a proposal of a structured hierarchy for documents in a security policy framework and how they should be approved and issued for use.

This study will also not discuss the content structure of different policy documents. Nor will this form any kinds of templates for the content or advice about the writing process.

The main restriction to this study was the lack of research in this area. My literature and paper search and research along with discussions with various security professionals did not identify any empirical research related to the security policy document hierarchy and its relevance to the organization. The literature offers an extensive amount of guidance about how to develop and manage security policies, but relating also a bit the area of documentation hierarchy. There have only been a few scientific studies targeting this area and even less scientific reviews on the policy hierarchy.

2 Development Method

2.1 Research Method

The research in this study started using constructive research as a method. The methodology is used in producing real world solutions to practical problems. According to Ojasalo et al (2009, 65) the constructive research method is suitable when a development task is meant to create a concrete plan or measurement or model. Constructive research is used to find a solution for a concrete problem via a new structure. In order to create a new structure, it is required to have a theoretical knowledge base as well as new information collected from the practice. Therefore, constructive research is aimed at finding a knowledge based solution to a practical problem which brings new knowledge to the function. Constructive research is planned where the model is implemented and tested. This research-oriented approach emphasizes interaction and communication between research implementers and their clients. (Ojasalo et al 2009, 65-66.)

Since the theoretical base was not available from scholarly studies, it was seen in quite an early stage of the research that the constructive research would not fit as the only research method. As the theoretical background was missing, it could not be used to test the theories. This meant that almost only theoretical background available was through literature and via such topics as policy development and architecture. For that reason, I focused on the qualitative data collection methods, which were a literature research and a survey (questionnaire). The literature study was done for getting knowledge about the views on the subject and to find out what kind of policy frameworks exist according to the authors and also analyze them. I compared those to needs Itella has. I also wanted to get the available theoretical background for this study. The background was used partly in a problem solving and also to help with other research methods such as with the questionnaire.

The constructive research method and its heuristic approach were used for the framework's gradual development and when testing the framework with tabletop tests.

I wanted to investigate the topic in a more structured way using an action research and the literature background. Basic qualitative methodologies such as questionnaires and interviews were used in getting data to be analyzed. The most important part of the interviews was the expert evaluations.

Expert evaluation or review as a method is more known to be used in user interface design, in software evaluations, and in usability testing. Software applications have been evaluated using this method for a long time and especially to find usability problems related to design and

implementation. The evaluation method is seen to be effective even when only three to five evaluators are used. Evaluation method Nielsen and Molich developed has been widely used and developed in different forms. Nielsen and Molich use the name heuristic evaluation about the model but also expert evaluation and expert review methods are used from the same kind of methods. Method contains readymade usability heuristics and researchers have developed heuristics further, and also new heuristics. (Nielsen et al 1990, 249-256). Action research method was also used when evaluating and validating the framework with phased research cycle and expert review process.

For example Nielsen's (Nielsen, 1995) one of the 10 famous usability heuristics for user interface design is like this: "Flexibility and efficiency of use".

Expert review method has been used also in other kind of research cases such as maturity model evaluation. Research paper from Puhakainen et al has used this methodology in gathering the most important characteristics for their topic area. They did it via survey and used subject matter experts to evaluate their model against these characteristics. (Puhakainen, Siponen & Karjalainen 2010). A similar approach and evaluation method has been used in this study to get the proposed framework validated empirically. Also tabletop tests were used to validate the framework after the expert review sessions.

Using all the findings I formed a proposal for a policy framework which would fit for Itella enterprise-wide and its organizational structure, as well as to other companies. I organized professional evaluation rounds with a few security professionals coming from different kinds of organizations where we reviewed my proposal towards the characteristics I got via questionnaire. Also, further development ideas were asked via questionnaire and via interviews during the expert review sessions.

2.2 Information Collection and Analysis

Collection of the research data was done using three different methods: (1) literature and research study, (2) an open questionnaire, and (3) expert review and interviews. The first part was the literature and scholarly study research. Various books from the different authors were studied to find out if a common view existed about the policy document architecture. The literature research was also done to give me an overall knowledge about different documents. During and after the literature research, it was seen that there is not enough academic research found in this area. Thus, I created an open questionnaire (Appendix 1) which was used to collect information regarding the view of the policy framework hierarchy, and what kinds of documents are seen as part of the framework. The questionnaire was sent to a group of leading security professionals in Finland.

The survey was primarily meant to gather information about the most important characteristics of security policy architecture. This information was used to find out if there is a common approach and view amongst the practitioners and what would be the characteristics of a good documentation framework and its structure. The characteristics presented and gathered were used to build, evaluate and adjust the security policy framework. The survey was also used to gather information about the current framework setting in organizations and what the respondents see as an overall logical structure.

After data collection, the policy framework was evaluated and tested using two methods: (1) expert review, and (2) tabletop tests. In the first phase, the security policy framework proposal was reviewed and piloted through an expert review process using security professionals as evaluators. After that, the framework was evaluated via workshop sessions held at tabletop test type exercises within the target organization. The created framework will later be implemented in real-life within the private sector corporate environment in Itella.

2.3 Strengths and limitations of the method

Constructive research and action research were methods which gave my research a systematic way forward. The strengths in this research culminate in using professionals with practical experience answering the questionnaire. I used the same professionals in expert review process evaluating the proposal. They gave concrete comments and ideas to think about. The same issue can also be seen as a limitation since in views, security professionals are quite a homogeneous group of people and this might lead to some streamlining of the answers. Expert evaluation as a method has been criticized about the fact that evaluation results are influenced with the knowledge and background of the evaluators. Organizations share information but also use the same consultants to develop policies and structures. That means that similarities spread, thus the framework has never been tested or proven functional. Is there enough courage to try new structural ideas when facing problems? Most of the organizations face difficulties in policy awareness and implementation as well as the maintenance of the documentation set. Could a new structure also help with this dilemma?

Using the questionnaire and interview conclude in the potential limitation of these techniques since keeping the subjectivity is an important factor. Not only could my own perceptions and views effect the interpretation but the respondents or evaluator's possible wrong perceptions or hidden motives could also affect the interpretation.

The missing scholarly studies plus the limited amount of available literature became a limitation to the scientific research in this study. Instead of the framework they are part of the lit-

erature emphasizes the content of the documents. It seems that my topic has not been studied before in any way.

3 Study of Research, Literature and Publications

This section starts the literature and scholarly study research. Various books from the different authors were studied to find out if there is a common view about the policy document architecture. Focus was also to find academic research around this common area. The reason for the literature research was also to give me a comprehensive knowledge about different documents in the framework and related important issues. Especially the goal was to find if the authors have the same kind of view about this topic area and compare the differing views. This knowledge is needed to design the framework and collect knowledge even further from the community of security professionals.

Rules and regulations are so common in society today that I thought from the beginning that quite a lot of literature and articles and even research would have been written on the topic. Even though the security policies are also widely applied in various organizations, and it has been so for a long time research around policy hierarchy is virtually non-existent. Literature is handling this topic to a certain extent and based on the literature there is a possibility to make an analysis about similar and opposite views amongst the authors. This topic is touched also in recently issued books, which might be a sign that a structured approach starts to be a new focus of interest.

In the following chapters the different views have been described on compiling a policy framework based on a literature review. The review will not focus on the content of the different documents and instructions about writing those. The review will concentrate on finding the justification and use for the different levels and document categories presented. The content is only mirrored towards statements being mandatory or just for recommendation.

Most of the existing literature and publications are guidelines on how the policies should be written, how many of them should exist and from what areas, and what they should contain. Also, a lot of policy templates can be found either free of charge or as commercial versions. These templates are not suited for any particular organization without adaption. There is also a risk of doing the bare minimum to fulfill some internal or external requirements where the fact that the policy exists is more important than the content of it. This should immediately rise following questions: Are these kinds of policies written for protection of the assets of the organization and are they been truly effective, or are they just a “tick in the box” exercise to address for compliance with regulatory or customer requirements? Policies have to be based on an organization’s business objectives and strategy.

Surprisingly enough, I found out that there are no commonly used policy frameworks documented in the literature. Furthermore, there is no common understanding of a structure for a

policy framework that could be found. This can be seen in the following chapters. It should be evident that some approaches work better than others, and this should raise interest to start to research this topic more in the research community.

3.1 Presentation of Document Types and Hierarchy in Literature

Policies define the organization's governance culture and objectives. They set the standard and definition for the operations of business processes and behavioral boundaries for individuals in the organization. The organization cannot really establish a strong security culture without policies (Rasmussen 2012). There are a lot of organizations who have gaps in their policy coverage, or they are missing the lower documents such as standards and procedures that really make policies concrete. The security policy framework is a structure for a set of documents designed to demonstrate the business's course of action to protect the enterprise and its assets. Naturally, it is an extensive development process to create the content of the documents and it is only part of the work since the implementation of those starts the real securing of the enterprise. Also maintaining and managing of the documents is a continuous process.

Normally, organizations have various types of documents in place in their set of directing documentation. Such types can be policies, guidelines, and procedures. Usually these kinds of documents do not necessarily exist in any particular order and/or they do not form a hierarchical structure. Furthermore, they might or might not inherit each other's views. The naming is arbitrary both according to their content and to their level of detail. When an organization lacks the control of their own governing documentation they might end up in a situation where instead of the organization's own needs being reflected in the rules, they are implementing rules coming from external sources such as auditors, customers or even material just cut and pasted from template documents.

The fact is that the business environment of today adds more and more regulation and demand for control to organizations. Politics and incidents change and add control via laws and statutes while for instance partnerships, outsourcing and the use of external services as part of the business's own functions make the same need for companies. The common belief is that the shorter the leash and tighter the control the better everything can be managed. Level of management and control should be adjusted based on the culture the organization has.

Organizations need to provide services to the customers either legally and/or contractually. Organizations management needs also to demonstrate that the business functions are conducted carefully while being compliant with the requirements, while still being able to practice due diligence. Without effective policies and their implementation the business objec-

tives cannot be securely and efficiently met. Development of policy documentation needs to start with the business needs and policy framework documentation needs to be beneficial to the organization. (Peltier 2004, 14-15).

Based on the literature review the guided hierarchical structures vary quite a lot. Sometimes this is about the naming of documents and sometimes they are talking about the definition of content. The following chapters go through the definitions and usage based on the naming of different types of documents. Also hierarchical aspects will be reviewed and handled when available.

3.1.1 The Intention of the Top Management

The security work in an organization has to have support and sponsorship from the management. The support has to be clearly demonstrated and the mandate for actions in the field has to be delegated by the board or the top management of the organization. This demonstrates the intention and need for support for implementing the security to the organization's strategy and therefore forms the base for all functions and activity that develop the security issues. A successful security development and implementation always needs some kind of documentation and actions demonstrating this management support and sponsorship. Also possible delegated authorities and mandates to certain functions have to be included.

According to Peters (2012, 7) there should be a Corporate Charter for security which would serve as the capstone document for the Information Security Program. He says the information security charter would define how the organization approaches security. Brotby (2009, 92) and Bacik (2008, 24) and many more on the other hand think that policies are the high-level statements and they do not mention any higher level clauses or documents from the management.

3.1.2 Policy

The American Heritage dictionary describes a policy as "A plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters" (2012). The same analogy can be used also regarding organizations' security policies which can be used to direct an organization or part of it.

According to Cannon (2011, 9) "policies are high-level documents signed by a person of significant authority", and that the signatory authority should have the power to force cooperation. Policies are stating that particular high-level control objectives are important to the organization's success and that they are mandatory to follow. This means that policies are

based on organizational objectives. The scope of the implementation will be determined by the person or authority of the area in question. (Cannon 2011, 9).

Brotby (2009, 92) states that the policies "can be considered to be the "constitution" of security governance". The same analogy can be extracted from Rasmussen's article where he states that "the organization cannot really establish a strong security culture without policies" (Rasmussen 2012). Peters (2012, 7) has the same idea when he states that "the policies are used to establish the holistic requirements and guiding principle used to set direction in an organization".

To justify their existence each policy and its content must have a specific business purpose. According to Peters (2012, 7)"policies should be used as a guide to decision making under a given set of circumstances within the framework of objectives, goals, and management philosophies as determined by senior management". There should not be a specific policy for every possible occasion; the number of policies should be kept reasonable. A good thing to think about is also that underlining documents such as standards are the documents which provide the lower level guidance towards achieving the compliance with policies.

Many references talk about policies in several tiers. For example Peltier (2004, 55) introduces three types of policies which are:

- Global policies (Tier 1)
- Topic-specific policies (Tier 2)
- Application-specific policies (Tier 3)

Senior management would be responsible for issuing the first tier global policies. The policies would establish the management direction in protecting organizational assets organization wide and those documents would be approved by a Security Steering Committee. A single senior manager or director would issue the second tier topic-specific policy. Those policies would be written to cover some current topic and the scope is one specific issue. Standards under one tier 2 policy can then support only this specific subject. (Peltier 2004, 10, 55, 64, 74). Both Tier 1 and Tier 2 level policies govern the whole organization and the Tier 3 policy focuses on one specific system or application, hence the application-specific and technical nature. (Peltier 2004, 74).

Organizations seem to have understanding about the meaning of policies as documents governing the behavior in the organization. The problem is that organizations combine policies, procedures etc. into one policy document from certain functional areas. This saves time but it is impractical and makes for example maintenance of the documents inflexible, and also understanding and implementing of them difficult. (Fitzgerald 2012, 143 & Peltier 2004, 50).

Different policy layers might cause confusion amongst personnel. Three types of documents named as policies as well as lower level documents are needed accordint to Peters. The document structure would expand quite a bit. I think the same outcome and still the same kind of flexibility can be obtained with a different kind of structure where documents are more obviously named differently and meant for a different level of information.

3.1.3 Standard

Standards are meant to develop the policies into operational requirements and limits. Standards can contain exact values to comply with or just limits or boundaries in which the organization has to keep within. With keeping policies on a higher level it helps to understand their difference to the standards and to the standard contents easier. (Brotby 2009, 110&115-116). According to Brotby (2009, 116) "the standards are the primary tool for setting measures by which policy compliance is determined".

Cannon (2011, 10) states that "standards are mid-level documents containing measurement control points to ensure uniform implementation in support of a policy". We can say that both Brotby and others have a similar view about the position of standards. Management identifies on a high-level "what to protect" by issuing a policy. Then the standards beneath the policies set the security baselines for the enterprise and its functions by defining the minimum security compliance limits. Security compliance of different functions can then be audited and measured against this baseline. This means that the operational governance is achieved via standards. Standards do not describe the workflow or working instructions on how to obtain compliance and can be considered as the "law" when talking about organizations security governance. (Cannon 2011, 10) (Brotby 2009, 92&116). This means that lower level documents are needed.

Even though the standards are usually mandatory some might also consider them to be best practices. Best practices are recommendations and a recommendation is not normally a mandatory practice. It is important to define the used terminology to prevent misunderstandings if there is irregular use of terminology. (Bacik 2008, 52).

Different kinds of standards can exist. Johnson (2011, 137-138) categorizes "two forms: issue-specific standards and system-specific technical or baseline standards". According to Johnson an issue-specific standard focuses on areas of current relevance such as the use of a new technological solution, or some issue which is concerning the company. Johnson sees system-specific technical and baseline standards as system specific secure configuration definitions. An example of such is a definition of a permitted firewall ports and allowed protocols. (John-

son 2011, 137-138). This kind of standard starts to be a low-level technical document prepared in cooperation with the respective specialists. I think that standards do not necessarily need different kinds of specialized types.

Standards have to be revised more often than the policies; they are about lower level specific issues which are easier to change. Also, the exception handling process can raise a need to update the standard.

Brotby (2009, 116) sees that a policy needs as many standards underneath it as there are classification levels in the organization. With classification he means classifications for criticality and sensitivity. He thinks the different classification levels are different security domains and that low-security domains will be less restrictive than those for high-security domains. According to Brotby "a typical governance structure may well have a hundred or more standards in three or four security domains". In his standard example he handles different classification levels within one standard, so maybe he does not truly mean different standard documents per classification levels. Brotby is the only referenced author used in this study who is thinking this way. Peters was saying the number of policies should be kept reasonable and I think the same analogy can be drawn to the standards.

Following the standards is mandatory even though the unit or group is not using for example standard equipment or current software. If they cannot meet the requirements of the standard, they must present alternative controls and standards. Those exceptions have to all be documented and agreed-upon. Auditing against the documents and assessment of compliance has to be possible. (Peltier 2004, 139).

3.1.4 Guideline

Brotby (2009, 92) thinks the "guidelines are helpful narratives in executing procedures including suggestions, tools, and so on". This is a bit of a different view on guidelines compared to other referenced authors who think the guidelines are on the same level as standards or even above them or straight under the standards. Still Brotby is also on the same page with others since authors such as Johnson (2011, 140) and Peltier (2004, 50) are thinking the guidelines help support documents such as a policy or standard. Many references imply that if standards do not yet exist, a guideline precedes it providing advice.

According to Johnson, guidelines are written to help in interpreting policies or standards and in assisting the organization in developing procedures or processes with best practices. They can also be written to present what the organization thinks about some current issue. He sees that the guidelines can be used to clarify a problem arising from the published policy or

standard. Following the guidelines is not generally mandatory, they are meant as guidance or a recommendation. Their writing is also optional when thinking about the security policy framework. (Johnson 2011, 140).

According to Cannon, guidelines provide advice on how organizational objectives might be obtained when there is not a standard. Cannon thinks (2011, 11) a guideline's "purpose is to provide information that would aid in making decisions about intended goals (should do), beneficial alternatives (could do), and actions that would not create problems (won't hurt)".

Key points to remember about guidelines according to Cannon are (2011, 11) as follows:
"Guidelines are discretionary because the directions provided are usually incomplete.
The user has to adapt or discard portions of the information to fit the intended use".

3.1.5 Procedure

In short the procedures describe specified steps and the process required in routine based activities such as audit tasks which is the same kind of process for every audit. Procedures are described in detailed actions, they must conform to the standards, and following of them is mandatory. (Peltier 2004, 50 & Brotby 2009, 92). Following of the procedures enables minimum compliance to a standard. (Cannon 2011, 11). Procedures can also be called work instructions. (Bacik 2008, 54).

According to Johnson the standards generally need multiple supporting procedures. The procedures are often documented by the same technical support personnel that actually have to follow those standards they are writing the procedures for. The security department may consult in the writing process. (Johnson 2011, 138). Wahe (2011, 34) is mentioning that procedures are usually incorporated into standards or guidelines. This seems to be different than the other referenced authors have referred to. This difference is due to the fact that others see that the parts with procedures would in these cases make other documents longer and also harder to maintain, which is unnecessary. The latter would also suffer due to the fact that the documents would contain very specific and detailed material, which would more quickly make the document out-of-date.

The reviewing of the procedures should be an annual process. It is important for ensuring the referred technical solutions are still valid and also if some optimization ideas have arisen. (Bacik 2008, 54). If a procedure proves to be ineffective, it should be updated by using the change control management process. (Cannon 2011, 11).

3.2 Comparison Summary

Since the subject of this thesis is not something which has been studied scientifically the plan was to compare what the different authors think about the hierarchy. The problem is that the hierarchies they present are just their own opinions about the subject area and the authors do not justify their selection for the document types or for the hierarchy they describe. The hierarchies are presented by the authors as a foregone conclusion. Literature is handling mainly areas such as subjects which the policies should be written about, how the policies are written or designed, what to include in different documentation content wise etc.

	E.g. Charter/ Code Of Conduct	Policy	Standard	Guideline	Procedure	Instruction	Tool, control, baseline etc.
Bacik		1.	3.	2.	4.	4.	5.
Baskerville & Siponen	1.	2.					
Brotby		1.	2.	4.	3.		5.
Cannon		1.	2.	3.	4.		
Johnson	1.	2.	3.	4.	4.		
Peltier	1.	2.	3.	3.	3.		3.
Peters	1.	2.	3.	4.	4.		
SABSA	1.	2.	4.		3.	5.	
Wahe	1.	2.	3.	4.	5.		

Table 1. Document type hierarchy analysis based on different literature references

I have made a comparison of the hierarchies presented by the different authors, which is presented in the table above (Table 1. Document type hierarchy analysis based on different literature references). There are not many conclusions which can be drawn from this table. Different views about the hierarchy order exist, but research about which one works best and in which kind of organizations does not exist. If we calculate just the average result from those differing views, we come up with the same structure as the top header line already shows. The only difference is that guidelines could be at the same level as procedures and that the instructions can be amongst the tools and such. It should be remembered that in real life, the lower documentation under polices sometimes needs references to more than one of the policies or to the other documents above or below them, or on the same level in the hierarchy.

The Sherwood Applied Business Security Architecture (later SABSA) framework is looking at the security policy framework a bit differently than the writers of the other reference litera-

ture does. The most significant aspect of the methodology is that all actions and in this case the documentation has to be derived from an analysis of the business requirements for security. When thinking about documentation SABSA's idea is that even the lowest document and its guidelines can be justified all the way up to the policies and business requirements. This idea also goes the other way around allowing traceability from top to bottom aka from business requirements all the way down through the stack of different types of documents. Traceability guarantees that all restriction and controls built for security has a business need that also has support from the management.

SABSA is a framework and methodology for Enterprise Security Architecture and Service Management and it is available to use without charge. SABSA has also been integrated to the TOGAF, an Open Group Standard, which is widely used enterprise architecture methodology and framework.

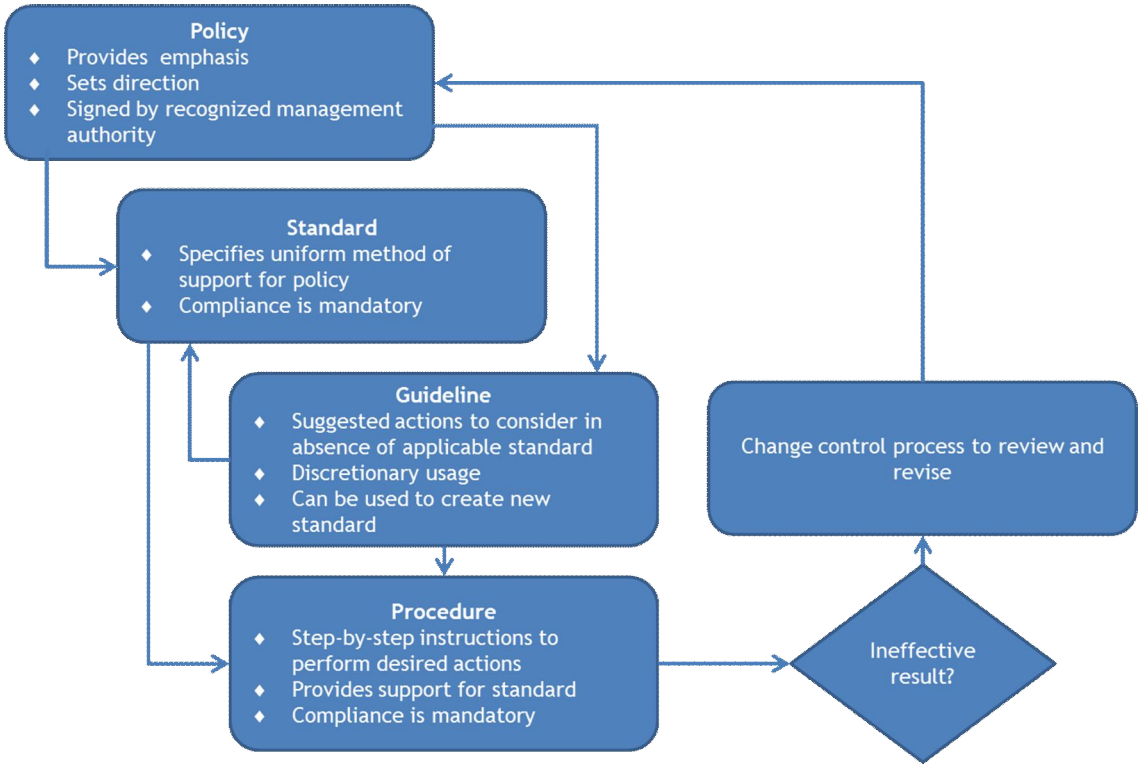


Figure 1. The relationship between a policy, standard, guideline, and procedure as presented by Cannon (Cannon, 2011, 12)

Cannon has listed typical document types used in the organizations. He has described the hierarchy quite clearly in the above figure (Figure 1. The relationship between a policy, standard, guideline, and procedure as presented) but the hierarchy is only based on the assumptions or his previous knowledge about document types.

3.3 Rules for the Documentation Framework

The foundation of the documentation framework is built by different standardized methods for defining documents of different levels. These methods were also studied from the literature since they were part of the scope for this study. During the following chapters, we look into the methods which are important from the framework point of view.

3.3.1 Document Naming and Revision

Johnson (2011, 157) emphasizes that the library of policy documents requires a numbering scheme which allows people to readily understand the context from it. A clear document naming structure will help to trace the document structure tree in both ways.

Johnson (2011, 157) presents a document organization as a tree growing sideways, where for example the information security charter forms the "root" for the tree. His thought is that the root delegates the authority for managing the tree to the information security department of the organization. Johnson would name the first document as IS (for information security), POL (for policy), and adds "001" as a number for the first document. The final outcome for the document naming would be IS-POL-001. Figure below (Figure 2. Policy and standards taxonomy library) shows the inherited naming structure. This policy framework what Johnson describes is based on ISO27002 topics.

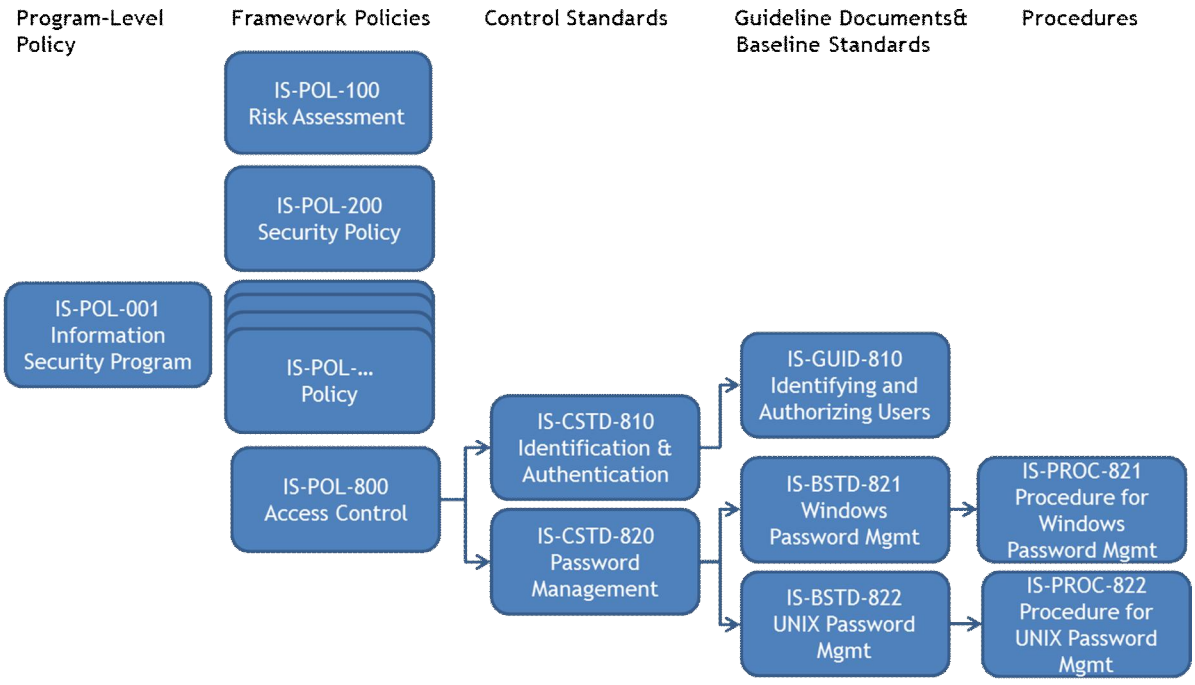


Figure 2. Policy and standards taxonomy library presented by Johnson (2011, 158)

There are not so many ideas about the naming convention in the referenced literature. Only Bacik (2008, 44) and Johnson (2011, 158-159) have examples of their ideas about the labels. It seems that there is not a standardized way to do a naming construction.

Conseil Européen pour la Recherche Nucléaire (later CERN) has published their document types and naming conventions for a certain project. They are project specific conventions, but their needs are similar as any other document structure. CERN needed the names to favor human readability but also computer readability and their focus has been on technical projects. (CERN 2011, 6). Their developed document name structure is visualized on the figure (Figure 3. CERN Project specific document name structure) below where LHC means CERN's project.

Figure 3. CERN Project specific document name structure (CERN 2011, 7)

CERN has strict format definitions for each field. Their own definitions are not relevant to this study but the idea of format definitions is. Policy style manual or metapolicy kind of document can include also standard about field formats. When documents are being written it would be useful to also use revision indexing and the text "-draft". This would be a clear implication of an unofficial version of a document still in development e.g. LHC-PM-QA-301.00 rev 0.1-draft; being first draft of a new document. (CERN 2011, 9).

3.3.2 Document Ownership and Approval

Ownership of the documents and the document approval process are handled quite cursory in the referenced literature. Brotby (2009, 111&116) states that "policies must be owned by the senior management and governing body, and the standards must be owned by the security management", but does not say which party should approve them. On the other hand policy level document ownership seems to be quite clear. Polices are part of an organization's foundation for security governance. Since they are high-level documents, they should be owned by the governing body and senior management. (Brotby 2009, 111).

Johnson (2011, 166) writes about extensive review processes for the policies and standards before they are approved and that they have to be approved by a senior executive. He thinks that the executive approver may be the chief information security officer (CISO) if the organization has that role appointed in the executive level. Peltier (2004, 116) on the other hand

states that policies have to be approved by management teams and does not make a suggestion for other document types. According to Johnson (2011, 139), the security department publishes procedures together with other documents once they have been approved but does not mention who approves the procedures.

One of the ISO/IEC 27001 (2005) standards control objectives can be seen as an objective of having a security governance body. The control A.6.1.2 says: "Information security activities shall be coordinated by representatives from different parts of the organization with relevant roles and job functions". Also Peltier (2004, 10) recognizes the need of the Information Security Steering Committee. His understanding about the participants of such a group is representatives from each of the major business units and the group chaired by the Chief Information Security Officer (CISO).

3.4 Document Lifecycle

The next few chapters go through some needed document lifecycle related methods and also conclude the literature review section of this study.

3.4.1 Development, Revision and Maintenance

The development of the documentation has to be done from top-down. Without this approach an organization will end up having a stack of "silo" type ruling. It will not form a holistic and a complete set of documentation. In this case, complete meaning that the areas needed to be covered are not covered fully to a needed extent.

All policy documents have to be created based on a need or a requirement. These come from the business, the environment where the business is done or from a process having issues or tasks needing standardization or guidance. More of these can be seen from the figure below (Figure 4. Internal and external issues affecting security policy contents). Without all this knowledge, policies may overlook some key issues and the organization could end up with an incomplete documentation set.

Figure 4. Internal and external issues affecting security policy contents

The documentation forms the foundation for the architecture and that is why they need to be thoroughly prepared as well as the cost and risk of each statement and requirement needs to be justified and tested. The purpose and objective needs to be clearly set so that all the content can be mirrored towards that.

The policies as well as the changes to them need to be approved and issued by an authority that has the mandate to take the decision of risks accepted and the costs of implementation which are consequences of the developed policy.

The policies should be developed by the request of the topic area's owner. The part doing the development and all the tasks of it should be given to a person or project organization that has a broad understanding of the topic. The more parties who have an interest of the final document, the more deeply thought it will be. There is though a risk of contradictory interest inside such project requiring a fast escalation.

A revision of the policy and its statements has to be done when external or business factors require such. Also if it is imminent that there are several places needing an exception from a policy, the whole sense with the rules should be questioned.

When preparing a document, it is vital also to put the more detailed statements and rulings in the lower level documents. This way the documents will have a longer life span the higher up in the document hierarchy they reside. The top document's life span should be compared to the corporate strategy life, while very detailed documents may be changed yearly, or even more frequently.

Many of the referenced authors have been writing that standards have to be updated more frequently than policies since the data in them expires easier. Peltier (2004, 117) recommends the standards to be reviewed at least annually. Standards are managed by information security staff meaning that requests for changes, amendments, and additions have to be made to the Information Security Manager. (Peltier 2004, 139).

All changes and updates to policies need to go through the same cost and risk analysis as done when a new policy is issued. The estimates of consequences may though be more accurate when talking about updates or changes, than they were when the original policy was made. To avoid unexpected consequences and avoid contradictory ruling when making changes to the documentation Johnson (2011, 172) recommends forming a policy change control board or committee. He thinks the board can either be a standing committee with regular meetings or a group which is formed when needed. This group would ensure the documentation is reviewed and refreshed when needed. Tasks for this kind of body are quite similar as with a Change Advisory Board when talking about Information Technology service management. The policy change control board would have tasks such as:

- Assess the documentation and make recommendations for change (RFC),
- Coordinate RFCs,
- Ensure the changes support the organizational goals,
- Review requested changes, and
- Establish a change management process for the document changes (Johnson 2011, 172).

3.4.2 Exception Handling

Many of the referred authors mention the need for an exception process. The exception handling process is needed when it is not possible to comply with the policy or the standard or other mandatory document. Even though the process is mentioned in the literature there is not concrete guidance for developing such a process at least in the referred literature.

Exceptions are inevitable. When there are rational and justifiable business reasons for deviations and when those are appropriately taken care of via an exception handling process the exception may be approved. (Johnson 2011, 40). Johnson does not mention or discuss who should take the expenses which are the direct result of the exception.

The exception handling process helps to keep the policy framework relevant and current. Especially when new policy or related documents are issued, and the organization cannot meet the requirements immediately, the exception handling process is vital. Given exceptions have

to be followed periodically since they should be granted for a predetermined time. (Johnson 2011, 139).

The exception handling process should be aligned and similar as the policy approval process. The handling should ensure that the business rationale of the deviation and determine if the exception is really necessary and needed (Johnson 2011, 40.). The acceptance of the exception may also contain conditions and complementary control methods which are needed to control the risk and keep it at least on the level approved in the original policy.

If a change control board or committee like Johnson suggests is formed, this organization is the natural point in getting information about all the exceptions made to a policy document. This way the organization might already, from inside, recognize and develop a need for a new policy change RFC.

3.5 The Literature Research Conclusions

Via literature research my understanding of this area as a whole grew and it gave me also a basis to start to develop the security documentation structure for Itella. Without the literature study it would not be possible to gain knowledge about the different views on the subject and to find out what kind of policy frameworks exist and analyze them. I compared the findings to the needs Itella has and used them when developing the framework proposal.

Without the theoretical background, it would have been difficult to start the qualitative data collection and design the questionnaire for the security professionals. The literature background is a necessary part in my investigations when using qualitative methodologies during the succeeding chapters.

4 Data Gathering and Expert Review Process

When it was imminent that an academic research on this topic area has not been really done, and that only literature is touching to this area, I created an open questionnaire. It was used to collect information regarding the common view of the policy framework hierarchy amongst the security professionals in Finland and especially to gather most important characteristics of a security policy framework for the expert evaluation. The next section will go through the process of conducting the survey and analyzing its findings. After that the expert review process will be described, and the analyzed and most important characteristics found will be used to evaluate the proposed framework.

4.1 Questionnaire

A questionnaire (Appendix 1) was used to collect information about the most important characteristics of a security policy framework among the security professionals. The questionnaire was also used to collect:

- Information about document types used in other organizations,
- What should be the document hierarchy,
- Who should prepare the documents,
- Who should approve and issue the documents,
- What kind of issues the document framework would affect positively or negatively,
- Also additional comments were asked.

The survey was made in Finnish and sent to 75 leading Information Security Professionals working in both the private and public sectors in Finland. Timetable for the questionnaire can be found from the appendix (Appendix 2). The response rate was 15 percent since 20 persons answered. I see this as a successful amount in times when individuals have to handle a massive information load every day and various questionnaires are piling in. The goal was also to get four to five respondents to agree on a short interview and an expert review process. I was able to select them among 16 volunteers who agreed to help me if needed. I based my selection on professionals having a position in the company which is able to influence to the documentation framework and also working in an international organization with multiple locations. The expert evaluation process will be covered in the next chapter.

The Security Professionals were asked their opinion about the most important characteristics of a security policy framework. The answers were analyzed to find characteristics which are proposed more than once and the following eight (8) were found (the amount of occurrences is told between parentheses): logical hierarchical structure (7), reasonable amount of hierarchy levels (6), ability to find documents related to certain role or task (5), all levels clearly

defined (5), no rules without justification (3), structure supports maintainability (3), clear approval structure (3), and part of common documentation structure (2).

Many answers were about the document writing process and document contents. Since this study is about the structure, those answers were not handled.

Document types in the organization and their hierarchy

The respondents were given a list of different naming of document types. First they were asked to pick the ones they have in use in their organization as well as put the types in an order of precedence.

It came clear that the meaning of the charter document was either not understood or known of it just is not in use in the organizations. I still think that most of the organizations have a charter-like document showing management sponsorship, mandate etc. Otherwise the question did not give any clear answers unless we look at the level given to the policy from the chart (Chart 1. The document types the organizations have in use) below.

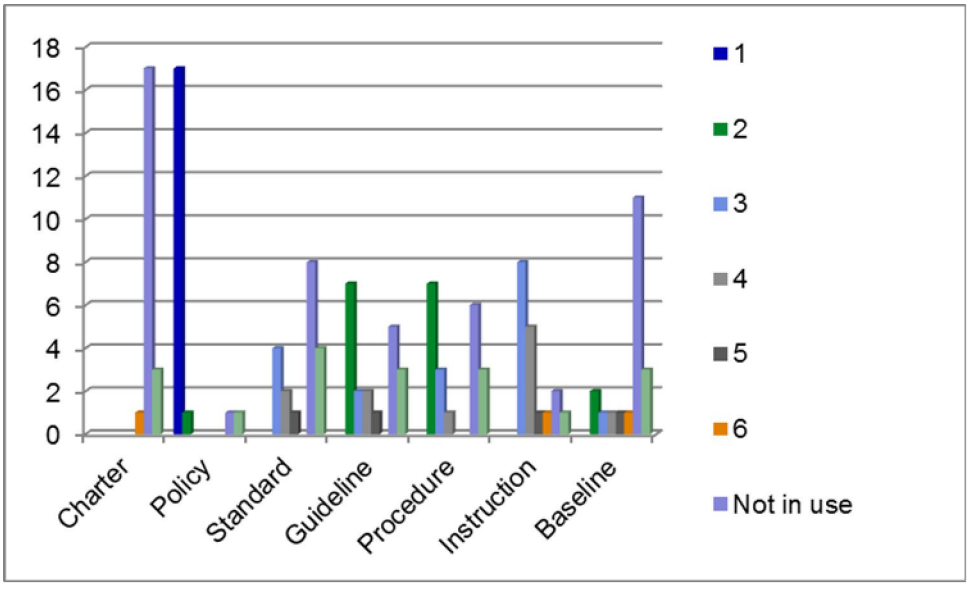


Chart 1. The document types the organizations have in use and their hierarchy

Respondents were also given the possibility to list their own document structures and give information if they use additional types of documents in their organization. Additional document types were Standard Operating Procedure (SOP), a handbook which can be seen as a baseline, various governmental documentation and norms, compliance table/matrix, principle (level 2), security manual for security function (2), manual (3), architecture (2), operational model (4), and sub-policy (2).

Based on the given answers it is possible to say that common approach on desingning the policy documentation framework does not exist among the respondents organizations.

Logical hierarchy for the document types

The respondents were asked also to mark the most logical hierarchical order for the given document types. The results of that question show somewhat scattered opinions about the logical order for the document types. The only clear differences give policies which should be first in the hierarchy and charter which isn't seen as a necessary part of the structure. The standard is seen as a second in the hierarchy by a few more than the third document which is the procedure. The guideline has been picked for every hierarchical level. Similar assumptions as with the previous chart (Chart 1.) can be drawn from the one below (Chart 2. Logical hierarchy for the document types). The organizations need a charter-like document showing management sponsorship, mandate etc. I think that maybe organizations have highest level policy for that purpose.

The document type "policy" seems in many answers to have a dualistic role. They see two levels of policy. One is a higher policy that dictates how the area and function is organized, and another is a lower level for dictating certain specific areas more thoroughly. The number of levels seems to be in some cases quite small, even though later the interviews showed that the perception of what is a policy document varies.

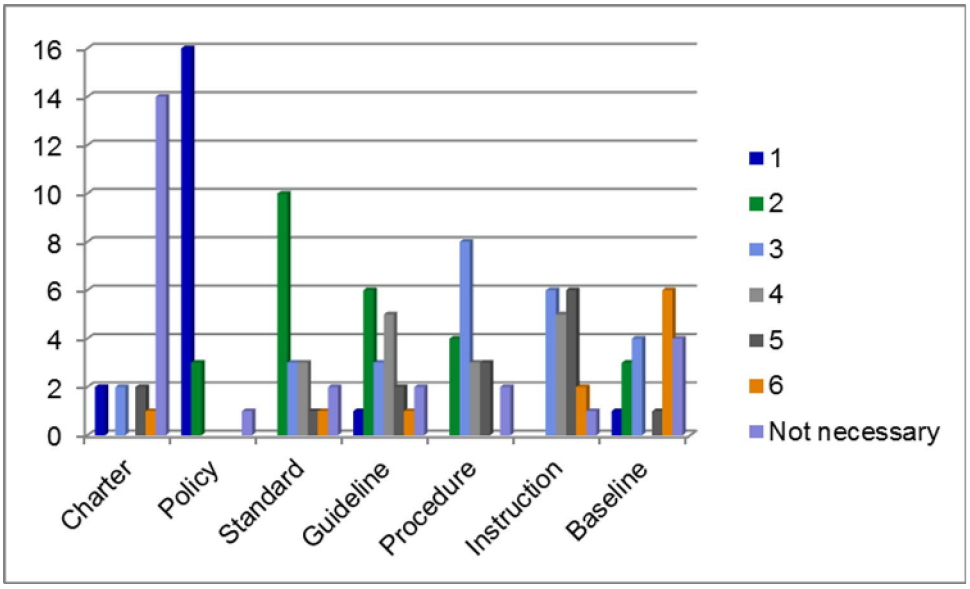


Chart 2. Logical hierarchy for the document types

The final conclusion really is that the current situation in the organizations (Chart 1.) does not give a common approach to the hierarchy and neither do the logically aligned view (Chart 2). So it is not possible to draw any standard or clear approach to define hierarchy from the given answers.

My assumption is that the latter (Chart 2. Logical hierarchy for the document types) corresponds more with what they want the hierarchy to be.

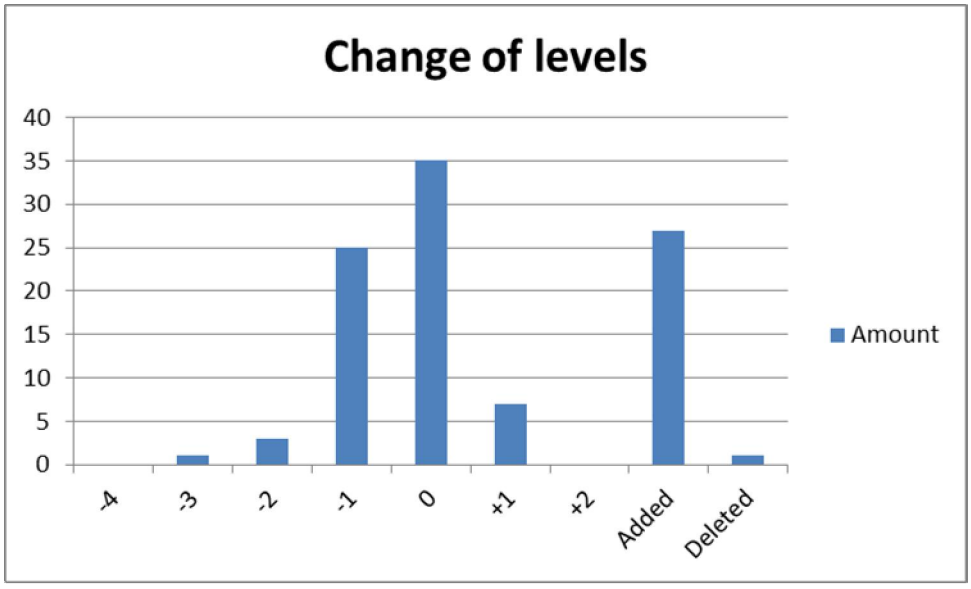


Chart 3. Respondents view of changing their current document hierarchy levels

In the above chart (Chart 3. Respondents view of changing their current document hierarchy levels) I have gathered the answers in a way where I have per respondent analyzed how they look at the hierarchical level of their current documentation compared to the question which hierarchical order would be the most logical one. Quite many changes seem to be wanted.

The questionnaire also revealed the respondents who have many document types in use where there is not a clear hierarchal place or order defined or the respondents do not have a clear picture about that. In total, 16 types of documents in the respondents' organizations do not currently have a specific level in the hierarchy. Since for the logical structure they have still selected the level for them I assume the respondents think they should be included in the hierarchy.

Looking at the cross reference of answers (Chart 3.) given there is clearly a contradiction in what is said and what is desired or thought as logical. The message from the respondents was that one characteristic of a good documentation system is that there should exist only a low amount of layers. On the other hand, many of the respondents want to add new types of doc-

uments when compared to their own current setting. Only one respondent want to reduce the number of documents, or they have found some types unnecessary for them.

I see that quite many want to make changes to the document hierarchy levels since 29 document types would logically have a lower hierarchical level when looking at the answers. Mostly, the need for adjustment is to lower the level of hierarchy of the documents. In only a few of the cases, the document type is thought to need a raise in the hierarchy.

This can be read so that most of the respondents think they do not actually find the current setting for their organization documentation hierarchy to be optimal. Not only new types of documents are needed and wanted but the hierarchy and the order of the documents also varies between the current and the one they are logically thinking to be the best one.

This result is also encouraging for me writing this study. It seems that there is a need or urge for some change, even though the respondents were not directly able to put their finger on this.

4.2 Empirical Validation of the Security Policy Framework via Expert Evaluation

The results from the questionnaire were used for empirical evaluation of the security policy framework. Evaluation and validation was done as an action research project consisting of one research cycle which contained four different phases.

The first phase of the research was to gather the characteristics which can be used for empirical validation of the framework. This was done with the questionnaire which was described in the previous chapter (Chapter 4.1). In the questionnaire the security professionals were asked their opinion about the most important characteristics of a security policy framework. Eight characteristics were extracted from those answers when taking into account only characteristics mentioned more than once.

The second phase was about performing expert evaluation for the framework and against the most important gathered characteristics. Four security professionals from different organizations did evaluation for the framework. Evaluations were done by one-to-one meetings with the evaluators. The evaluators were from different multinational companies: (1) a chief security officer (technology services industry), (2) an information security architect (energy industry), (3) a chief security director (logistics industry), and (4) a security program lead (telecommunications industry). Each evaluation session results were recorded by the observer via writing down notes of the comments the evaluators made when going through the framework structure proposal (Figure 5. Evaluated security documentation structure version) which was

developed based on the gathered knowledge from the literature research and the questionnaire. Timetable for the evaluations can be found from the appendix (Appendix 2).

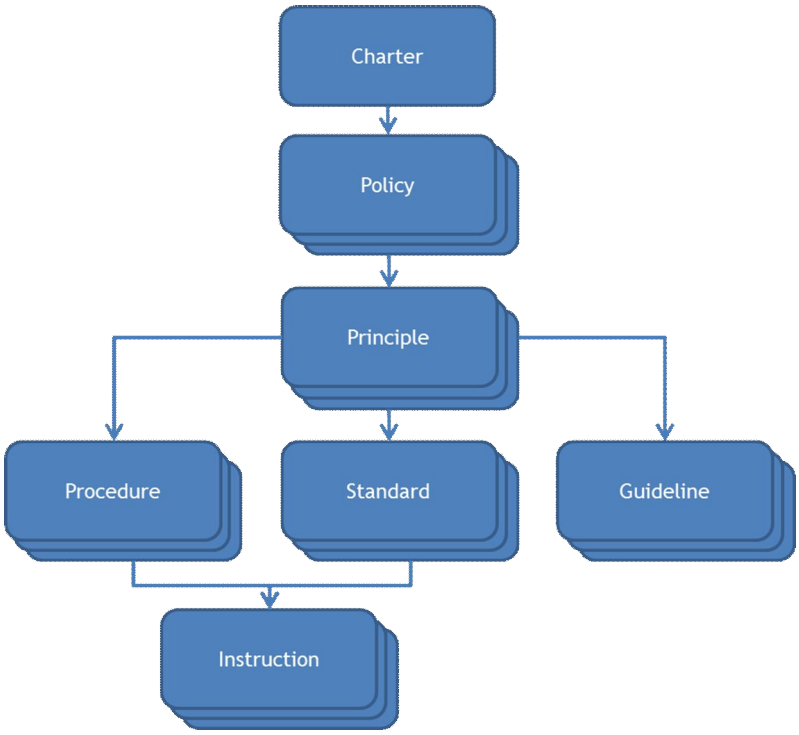


Figure 5. Evaluated security documentation structure version

The evaluators were asked to reflect on the framework against the gathered characteristics when going through the proposed framework figures, (Figure 5. and 6. Evaluated security documentation approval structure version) and also to express any additional comments or development ideas.

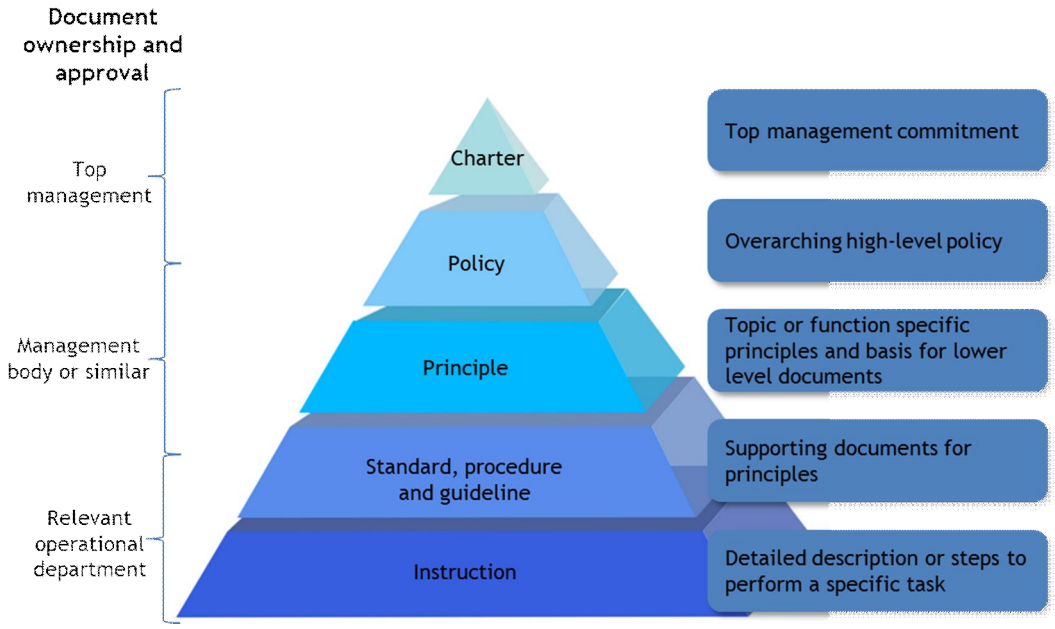


Figure 6. Evaluated security documentation approval structure version

Every evaluator also shared information about their own documentation structure and answered a few pre-defined questions. These included such questions as:

- Do you have a document naming structure and which kind?
- Is your security document structure part of organizations normal document structure?
- Are you security documents available with a role based search?

The third phase was about how the characteristics and framework co-exist according to the evaluation. It was seen before the evaluation that some of the characteristics cannot be evaluated based on the figures of the structure. Those are:

- Ability to find documents related to certain role or task,
- No rules without justification, and
- Part of common documentation structure.

The above characteristics are good to take into account when writing the documents and when organizing and publishing them, but those are not parts of the structure. Itella does not have a common documentation structure. This security document framework can be implemented also as a common Itella documentation structure and it has been developed with that focus in mind. The framework evaluation was finally done against five characteristics in total and the above mentioned three were only discussed.

After seeing the first evaluator's presentation about their three tiered documentation structure I was already anticipating the following comment:

"The structure contains too many hierarchical levels. Otherwise it complies with the heuristics."

The second evaluator did not confirm the argument the first evaluator made about the levels:

"The documentation framework complies with the heuristics. Our organization has similar documentation structure and it is being developed even closer to the proposed one. The amount of hierarchical levels is appropriate.

Avoiding conflicts between the documents requires work which should be taken into account. Update process has to put effort in checking cross-references and keeping the structure together. Changes to one document have a wide impact."

The third evaluator had not heard about principle as a documentation type. The evaluator confirmed the argument the first evaluator made about the levels and also gave other comments:

"There are too many hierarchy levels for corporate level security directives. All levels are defined but not clearly based on evaluation of the pictures. Clear definition would need about two pages decription per document type. Security practices should be refined from security specific documentation to other common documents (e.g. project guidelines). Other characteristics seem to be complied with."

The fourth evaluators' comments can be seen fairly positive:

"The documentation framework complies well with the characteristics and the structure can be seen as a logical one. Need for different documentation types can be seen but especially the lower document types require a clear definition to help understanding the difference".

The fourth phase was about improving the framework according to the evaluation. Compliance against the characteristics was evaluated to be mainly positive and encouraging. The evaluation suggestions to limit the hierarchical levels were a good critique since it really put me into thinking once again is there too many hierarchical levels in the framework or not. That also encouraged me to put more effort into the framework case study to see if adjustments are needed and the view the tabletop tests would give. Comments about too many hierarchical levels were also contradictory, since when comparing those comments to different parts in the questionnaire, the results were not indicating a need to decrease the number of hierarchy levels.

Also the lower level document types, which were criticized by some, are actually in use in some of those organizations too. They do not necessarily have the types of names used in this study and they might not officially be a part of the document structure and layers, as I have described. For example instructions are often seen as an additional document type not part of the official structure. The fact is that the lower level documents can and must be written in almost any part of the organization, but as I see it, they should still link to the higher ones and be a part of the structure all the same.

The effort should be put on describing the different types of documents clearly in the organizational guiding document for the usage of the different types. Also, the maintenance process should be described in detail and it must be ensured that the impact of the changes is assessed fully when they are made.

In a few of the answers from the questionnaire the respondents stated that security documentation should be part of an organization's common documentation management and structure. The same idea was discussed with the evaluators who all agreed with that. I cannot agree more and I can fully support this. Since Itella does not have a document management structure, my perspective for developing a structure for security documentation has also been to create a structure that could also be used as a general document structure for the organization.

Improving the structure

After the expert evaluation session, the security documentation structure (Figure 5.) went through minor adjustments. The structure itself was kept the same since the evaluation sessions only strengthened the proposed idea of the structure as being the one to proceed with Itella. In the middle of the evaluation sessions, and based on the comments I received I added information to the structure about the documents which are mandatory and which are recommendations. Also based on the discussions it came evident that standard can refer to the guideline and to the procedure and also vice versa. For that reason, double arrows were added between standard and guideline, and between standard and procedure. The adjusted figures can be seen when going through the following chapters.

Also, the evaluated security documentation approval structure (Figure 6.), where the structure was described with a pyramid picture, was specified a bit. Only braces scoping the approval levels were specified more and otherwise it remained as it was. It was seen when discussing with the security professionals that the approval structure should be based on the same as organizations normal management structure as was suggested.

5 Developing Security Policy Framework for Itella

During the following chapters all the researched data and the gathered knowledge is merged in the Itella specific development ideas. These chapters start with describing Itella as an organization and its history with policy documentation types and their approval structure. Also recognized need for this development is described. The main focus on these chapters is still the actual security document framework proposal which you can find from the chapter 5.2 onward.

5.1 Itella as an Organization

If the organization does not have a sound security policy framework, it might be possible for externals such as auditors to come and set their policy for the organization. Itella's goal is to establish their policies from their own business perspective instead of having an "outsider" laying it out for them. Itella as any other organization is required to provide services to the customers legally and according to the contracts. Security work is not done for security's sake; its focus is to support organizations objectives.

5.1.1 Background

Itella is an international service company which offers a wide-ranging set of services specializing in customers' important information and product flow management. Those services are offered from its three different business areas as own companies. They are later referred to as Business Groups: Mail Communication, Information and Logistics (Itella Corporation 2012, 1). Itella is a public limited company 100% owned by The Finnish Government and it operates in Europe and Russia.

Itella Logistics provides service logistics solutions. These solutions include road, sea and air freight, warehousing and other contract logistics. Itella Information offers solutions for sending sales invoices and for processing incoming purchase invoices. They also have automated cash and treasury management solutions and outsourcing solution for financial transactions. Itella Mail Communications is the only provider of 5-day regular mail delivery services in Finland. For businesses, it develops new, multi-channel solutions for targeted marketing. In Finland, they serve consumer customers under the Posti ("Finnish Post") name. The organization chart can be seen in the figure (Figure 7. Organization chart for Itella) below.

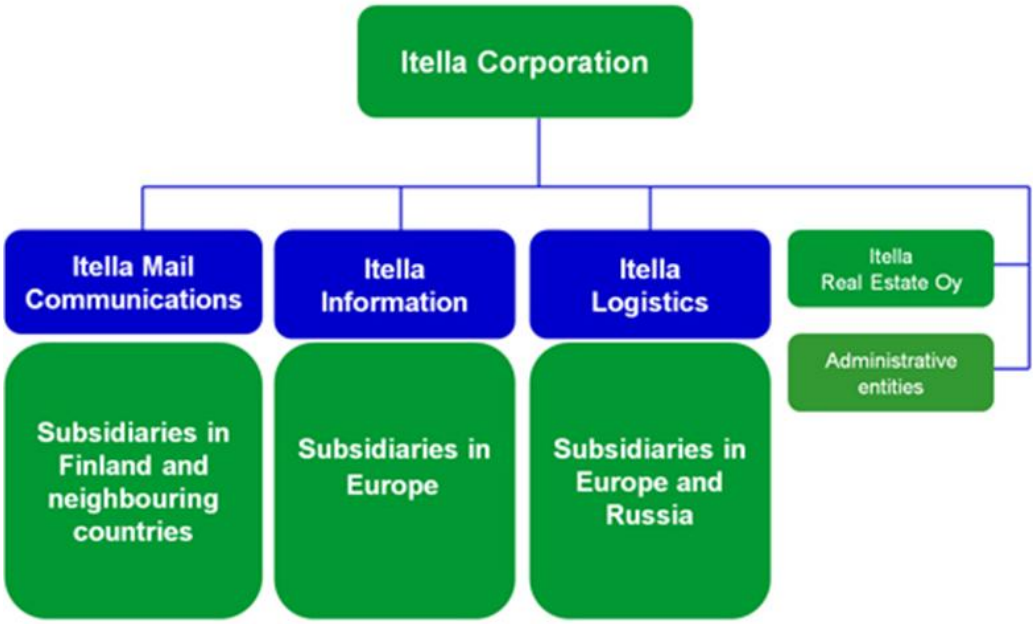


Figure 7. Organization chart for Itella (modified Itella 2013a)

This means that Itella handles assets in different forms owned by other individuals and organizations. Examples of those assets are paper mail, electronic invoices and parcels. Itella also handles many other kinds of sensitive information on behalf of others. This is an act of trust and demands responsibility from the whole enterprise. This also means that there are different kinds of security needs and requirements among the enterprise functions along with the ones Itella has. Itella policies set a baseline for security for the whole corporation. When for example one Business Group has needs to raise the security level from the baseline there follows a need for different versions of the polices or other documents. All of those should still be connected to each other's.

Itella does not have a formal procedure for security policies or their development and approval. The policy development and approval process depends on the topic area and the case in question. Still, the top-level policies such as corporate security policy and information security policy have been approved by the CEO of Itella Corporation and by this the policies should be followed in the whole Itella. Currently the Business Groups of Itella do not have any of their own security policies. They have documentation such as instructions and process descriptions which can be seen as part of the framework. The whole Itella still lacks much operational and low-level documentation such as standards and procedures that really form the policy framework.

Security related sub-policies in Itella have been formed mainly by the Corporate Security function and reviewed through and commented by the corporate-wide Information Security Virtual Team (later ISVT). ISVT has members from all of Itella's Business Groups, and central

Itella companies, as well as the Corporate Security function and Itella Corporate ICT unit. After the review process the Information Technology related policies have been taken to the Information Technology Executive Board (later IT EB) to get a corporate level approval. Also other respective Itella Boards have acted as approvers. Some of the policies are approved in Itella Executive and Management Board (EB/MB) level.

IT EB is not a decision authority itself, but it advises the corporate Chief Information Officer (later CIO) and uses the CIO's decision rights. IT EB is comprised of the IT Heads of each Business Group, Directors of Corporate ICT and the CIO who chairs the IT EB. Strategic IT decisions are made by the IT EB in line with Itella Corporate Strategy. ISVT has officially earlier been named the IT security virtual team and the team has not been formalized as part of the IT Governance model in Itella. When we look at security and information security as a whole, I would not recommend it to be part of IT Governance since it narrows down the handled issues too much to IT and technology specific areas. Certain issues may be common with ICT and information security, but for instance process enhancements and building security into those might become out of scope within ICT governance. This difference will be covered in the next chapter in detail.

The process of approving documents in this current organizational composition is slowing down the decision-making when documents containing detailed sections or low-level documents need to be approved by a high-level organizational body. Current policies contain very detailed areas where high-level bodies do not have the necessary expertise. Bringing up these kind of documents for approval on a higher level, would only become a time consumer due to meetings, and thus creates annoyance for the attendants. This could also have a consequence which would be contradictory to the whole cause of security.

5.1.2 Current Security Organization and Policies

The information security is often seen as a synonym to IT security and therefore only a technological issue. Information exists and is handled in many forms, places and processes, not only in IT systems. Computer-held information comprises a small percentage of the organization's information resources. Guiding documentation and information security efforts should therefore cover all forms of information and processes handling it. (Peltier 2004, 53&55)

According to the Corporate Governance Task Force (2004, 5) "information security is not only a technical issue, but also a business and governance challenge". They see the security governance as a subset of the organizations' overall governance program.

Information Security is much less a technology issue than a management and governance issue. A Swedish research made by Johansson et al (2006, 3) came up with percentages for information security stating numbers such as 36% for technology and 56% for organizational issues. The exact numbers can be argued and are impossible to determine, but at the same time they are unimportant. The main issue is that the governance documentation which forms the foundation for management and governance of security are profound and crucial for building and implementing security.

Today, the Itella corporate security policies define the security baseline. Possible exceptions should be handled by the management of the respective Business Group. There are no guidelines on how to organize the exception process and how to handle additions or raises to the baseline and to their documentation. There are also no guidelines on how to process Business Group level sub-policies. The naming documents as a "policy" have not been restricted to any certain level documentation or content. The process how the document is formed, approved and issued has not had any influence on naming. This means that that the term is in use in various types of documents across Itella.

Current security policies have some sort of lower level documentation defining issues in a more detailed level and there is also a growing need for specifying issues more thoroughly. Existing security policies handle their area in too detailed level. There are different kinds of guideline documents specifying information security related instructions. Still there are no specific rules which would tell what kind of documents there should be under a policy or which kind of documents there can be and how those should be reviewed, approved, updated, and by whom.

5.1.3 Recognized Need for a Structure

Today Itella does not have a general document structure that is supporting the objectives presented. One attempt is the Itella Way Handbook. Some years ago there was an effort in Itella to collect all of the top policies and guiding documentation to a single source and document. The aim was to build a binding description of the international management system for the whole Itella. This was a single and common way of working. This was called the Itella Way Handbook. It was built as a joint effort with subject matter experts and different area owners adding their part to the document. This document, unfortunately, has been kept neither current nor reviewed to an extent needed, which is why it has slowly fallen back and lost its meaning. It says a lot when even top managers are totally unknowing about the existence of the document. The document was the foundation for "One Itella", as the slogan said. The projects to unify the working routines have continued even though the guidance documentation lags behind.

The Itella Way Handbook practice though has not followed any principles, which have led to the current situation with a lot of documents called policy containing material of very different levels. The order of precedence as well as the issuing body of the documents is not clear.

The situation is not in any way enhanced by the fact that Itella lacks a general and common document management system, meaning that all the documentation is scattered not only around the different parts of organization but also in different medias and places. Most of it should be in electronic format somewhere.

Itella has an intranet where most of the documents can be found. What is lacking is a general way to find the correct ones, and to know directly if the searched and found document is relevant for the searched role or situation. It is also unclear whether or not it is the most current or up to date version.

As the current document storing and issuing environment has been developed by itself during the years it does not support a clear structure. This has to be built into the documents themselves and begins with their naming and use of clear level thinking.

Even though Itella has a need for common organizational documentation structure the scope of this study was to form a documentation framework only for the security documentation. Focus has still been to find a framework which would also work as a common structure.

The organization structure of Itella gives the development of the hierarchy its own difficulties. The structure of the organization can be seen in the page 42 (Figure 7.). Even when Itella seeks a centralized policy management and ownership model it must allow to also form decentralized documentation to further refine the requirements and statements. The same policy should be able to have different versions since different Itella Business Groups may have different requirements as well as within the same Business Group different versions may be needed based on localization of type of service provided. Those documents should also be known and connected to the other documents in the framework.

Common for the whole Itella is one of its declarations to take responsibility openly and reliably. Itella declares its principal task is to produce services required by the community by securing its customers' important information and product flows. One of Itella's corporate responsibility principles is that Itella processes all information and product flows securely and in confidence. (Itella 2013b). This means working security governance is a crucial part for the whole enterprise and a clear business requirement.

5.1.4 External regulations

External regulations within the context of the Itella Policy Framework refer to any external legislative mandate, regulatory obligation, and industry requirement facing the organization in their operating countries. Itella has also chosen to comply or follow such regulated frameworks as Authorised Economic Operator (AEO[1]), but also security frameworks such as Transported Asset Protection Association (TAPA[2]), Information Security Forum Standard of Good Practice[3], and ISO27001[4]. Some of Itella's Business Groups and/or functions have framework based customer agreement requirements such as Finnish National Security Auditing Criteria[5] (KATAKRI), and Degree on Information Security in Central Government[6] (VAHTI tietoturvatasot).

These external regulations do not guide how the policy framework itself should be structured; they set requirements which should be taken into notice in the contents of the documents within the framework.

5.2 Document Type Proposal for Itella

Itella level policies are the security baseline for all organizations that are part of Itella and they must be followed everywhere in the enterprise. If Itella Business Groups or other companies in Itella need to have specification to the baseline like more stringent requirements, they can issue their own versions of Itella level security policy framework documents adding more business specific requirements. Also, specifying mandates and roles within the Business Group might be needed.

It should be known that implementation of the security policy framework should never be done only to satisfy external audits or security requirements. The whole framework should be

---

1 http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/aeo/index_en.htm

2 http://www.tapaemea.com/

3 https://www.securityforum.org/

4 http://www.iso.org/iso/catalogue_detail?csnumber=42103

5 http://www.defmin.fi/?l=en&s=637

6 http://www.vm.fi/vm/en/04_publications_and_documents/01_publications/05_government_information_management/20101028Instru/name.jsp

built based on business objectives and the mission of the enterprise, and it is done for running the enterprise efficiently. (Peltier 2004, xxiii).

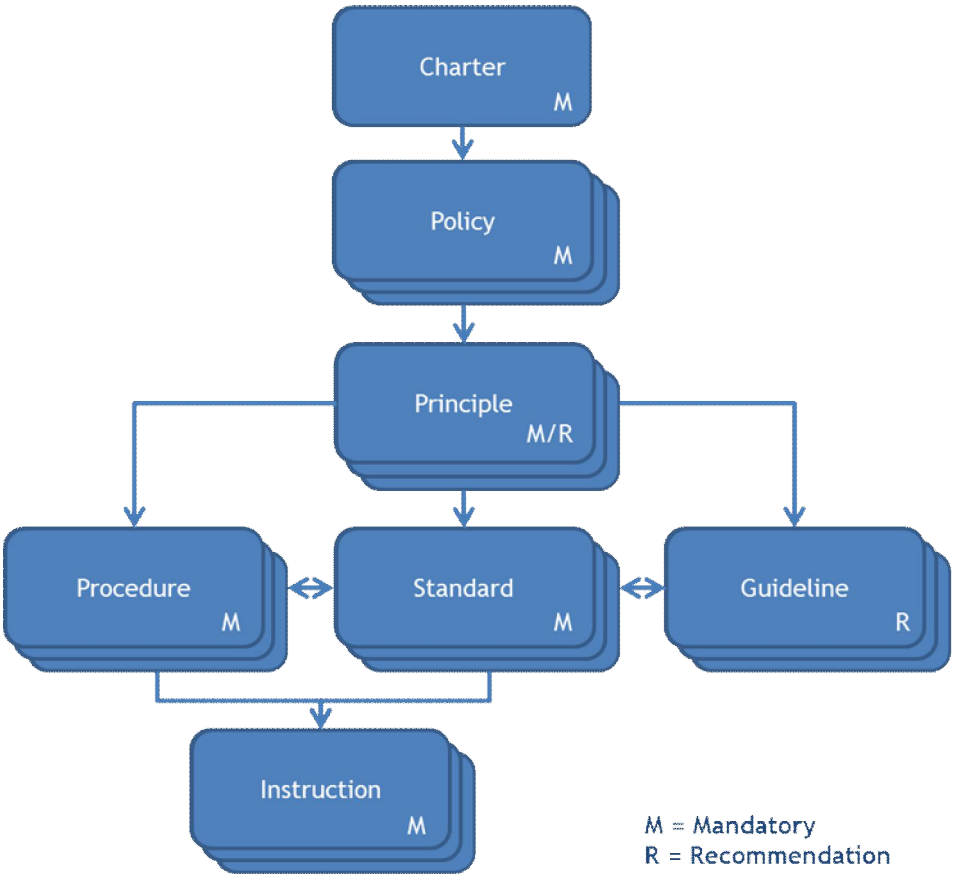


Figure 8. The security documentation framework proposal for Itella

A graphical presentation of the recommended proposal for Itella specific security documentation framework structure can be seen in the figure above (Figure 8. The security documentation framework proposal for Itella). The reasoning behind selecting this structure and the thought content for different document types can be found from the following chapters.

The proposal was developed from the original version based on a few comments which were given via expert evaluation and interview sessions. Now the figure contains information about mandatory document types, and types which contain recommendations. Principles contain generally mandatory directives, but they can also contain recommendations. It depends about the wording of the clauses which ones they are. This topic is covered in detail when describing the principle document type in chapter 5.2.3.

5.2.1 Charter

By issuing and signing the corporate charter the Itella Corporate CEO sets the basic steps and directions for development by drawing the lines of intention for the whole Itella. The charter provides strategic guidance to steer the whole security development work. The charter also dictates the top structure and mandate for different policy level documents as well as emphasizes the meaning of the directive documents. It also focuses on the code of conduct and how it reflects on the security guidance.

In the charter document, the exceptions to rules are also defined to be unwanted and the formal process to the exception handling will be justified.

This kind of document does not currently exist in Itella but instead similar content is in the corporate security policy and information security policy which both have been approved by the CEO of Itella Corporation.

Besides the Charter, the business objectives can be found from various documents such as the Itella Corporate Code of Conduct, the publicized strategy paper and Annual Reports. All signals help to ensure that the focus of the security documentation supports those objectives.

5.2.2 Policies

The policies concretize the content in charters. Different areas and responsibility functions have their own policies. In policy named documents the accountabilities, rights and responsibilities within the function as well as how the function is organized within different parts of the organization are described. The policies are binding and mandatory in their nature.

Areas or functions having an own policy could be such as security, including information security, business continuity, crisis management, risks management, communication, human resources etc.

The security policy is thought to contain opinions about key points in its area along with the rights and responsibilities for positions and the governance inside the function. The policy documents should be kept high-level, short and precise documents.

5.2.3 Principles

In many organizations, policies have been expanded too lengthy documents or they are issued in several hierarchical levels or tiers, as for instance policies and sub-policies. Policy tiers

lead to several documents of which the internal hierarchical order cannot be clearly determined by its naming. Tiers and levels are demonstrated and made understandable by a clear structure. If this structure does not exist, a vital part is missing. Besides this, the naming of the documents does not in any way support the visualization of the structure.

When the current situation within the documentation in Itella is such that policy document type or just naming of the documents as policies has spread documents in various levels I feel it is clearer to introduce new document type in the middle of policies and standards along with new highest level charter document. My suggestion for Itella is that the lower level policies should be renamed as principles. The document type will clarify the level of the document. The statements and requirements are, depending on the content and phrasing in statements, either mandatory, a recommendation or optional.

As the term Principle both as a word in dictionaries and in use in some organizations are treated similarly as the word policy, I see that it can well be the document guiding the policy implementation in different narrow fields. This is done according to the fields and issues that have the need for further steering documentation. Principles also ease the current pressure of expanding the policy documents too much. The principles are thought to function as a similar document category as specific functional security policies which seem to be a better known and used document type. These are a kind of traditional security policy document which handles specific organizational requirements in appropriate detail.

Principle is not a new document category in Itella even when its role has not been as official as I am proposing. Current Itella Way Handbook which was mentioned in the chapter 6.1.2 uses the term principle in various occasions and talks about policies and principles. This is quite natural additional document type to the Itella policy framework.

If we look into the European Union Data Protection Act and how it is regulating the use of "personal data", we can see that the Act requires protecting data by using principles in the Act. Based on the literature research, principle as a term in security documentation naming is less known and used. It is still often used when discussing mandatory directives in the organization such as a principle of least privileges. I see that this can be used instead of different policy related document names such as sub-policy.

Principles are documents describing the issue and controls to be used. The controls, components used and methods described are either set to be mandatory or as a recommendation. The fact of what the issue is can be determined from the wording and phrasing used. The verb used in requirements and statements controls the meaning as follows: if the word "must" or "have to" is used then the following of the requirement is mandatory. On the other

hand if “would” or “should” is used then we are talking about a recommendation. When the term “may” is used in this context it refers to an optional condition.

The principles form the baseline for the requirements and together with their possible mandatory complements of documents below them; they therefore also form the base for internal audits within different parts of the organization and within their functions.

5.2.4 Standards

Standards should be part of the Itella policy framework since they are the exact tool to give the tolerance limits where the organization has to function.

Brotby (2009) was describing the idea of different standard documents per confidentiality and sensitivity classification level. I do not recommend that approach to Itella since the policy framework would become too complex when layer of standards would expand too much. Since the whole approach to the documentation framework will be renewed, it would be better make an easier and more understandable transition from current documents to the new framework. Brotby was the only referenced author who was recommending this approach. There should be more studies available from his approach to convince me to recommend his ideas about standards. Still I would recommend Itella to keep this idea in mind when classifying assets. Do different classification levels need different requirements and can they be in the same standard? I think that mostly they can be handled inside the same standard and I give a recommendation about an approach to this in the document metadata paragraph 4.4.2.

Standards are mandatory tool or implementation, as well as form that is to be used in all cases they apply. Bacik (2008, 52) is describing that even though the standads are normally mandatory, some might consider them to be best practices. This should be clearly specified that Itella standards are not best practices and that the guidelines exist for that reason.

Standards have to be revised more often than the policies and principles; they are about lower level specific issues which are easier to change. Also, the exception handling process can raise a need to update the standard.

5.2.5 Procedures

Since standards do not describe the workflow or working instructions we need also procedures which could also be called Standard Operations Procedures (SOP). The procedures form the standard of doing and acting when talking about processes and missions. The procedures usually contain several steps for fulfillment, but this is not necessary.

As procedures are standards of their nature, thus being for instance mandatory, this could have been left unchosen in the framework. However, I wanted to keep it there as a complement to stress the fact that the content of it refers to a process or an act of doing.

The procedure describes the detailed steps required to implement the standard or principle. They are used for the procedures which are conducted the same way every time. A person following the procedure should not need to look at what the policy or principle is saying. When following the procedure, the actions are done as they should be done automatically.

5.2.6 Guidelines

Guidelines support principles as statements given for recommended or preferred actions. The guidelines are often more generic leaving more space for interpretation. Guidelines are also used to specify statements in principles to be applied for different situations. For example, guidelines can be used by development projects to help the project management to do a risk assessment of the project. The guidelines can also refer to specific mandatory (standard) tools to be used in certain situations. But as per definition the guideline leaves the responsibility of the implementation to the part using it.

Guidelines as a document type are needed to be used as handbooks for certain general situations, for which the principles need to be applied even though a direct or clear implementation of a principle cannot be made.

5.2.7 Instructions

Instructions are short descriptions for particular tasks to further and very specifically describe and complement the content of standards and procedures for a certain situation. This can contain small ways of implementing or act like installation instructions; instructions on how to make a report on a security incident, instructions for a security officer how to do a certain task and so on. The instructions can also be formed as work orders, as please do XX to YY according to instruction ZZ. More concrete, this could be a work order to create an account to person NN or change the backup tape in slot 24 and take the old tape for storage. The instruction then contains the steps that have to be followed precisely.

Instructions might not normally be described to be part of the documentation system, even though they need to fulfill and follow all the guiding documentation. By adding these as a part of the structure and implementing them as full members, they also become a part of the management and review cycle. This is also especially important when employees in different

tasks change and new ones need to be taught the routines. If the instructions are haphazardly here and there, there is no guarantee that a new person can or will be able to work correctly in her task and comply with them.

5.3 Two-way Traceability

The whole security documentation framework should be about analyzing the business requirements and done for supporting organizations objectives. The documentation structure should support traceability of the solutions and decisions and chosen ways of implementation (top-down) and also support justification of the solutions and decisions in the guiding higher level documents (bottom-up). This can be partly shown with the clear hierarchical documentation structure which shows the order of the documents clearly. The document naming structure would also help somewhat in finding the path from top-down or bottom-up. Still the content of the documentation structure is the most important factor when keeping the traceability and justification factors in place. Also references to higher and lower documents should be included in the document to support the traceability.

Two-way traceability guidance can be found from the SABSA framework (Sherwood et al 2005, 88). The framework guides to assure that business requirements for security are met and the residual risk is acceptable to the business appetite. This means that the traceability for completeness is assured (Figure 9. Traceability for completeness).

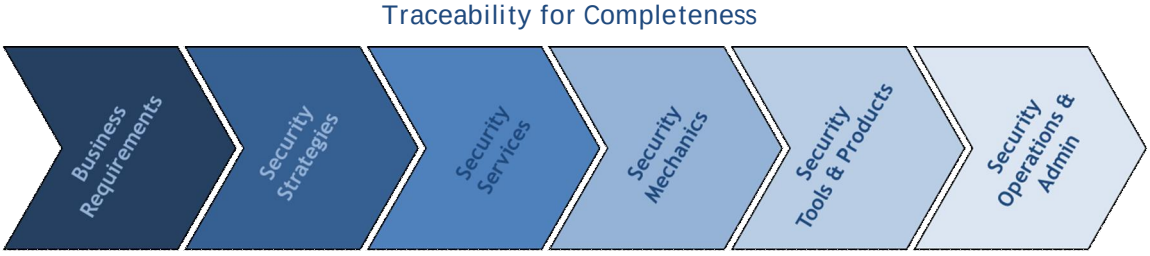


Figure 9. Traceability for completeness (Sherwood et al 2005, 43&88)

The SABSA framework also guides to assure that every operational or technological security element can be justified by reference to a risk-prioritized business requirement. This means that the traceability for justification is assured (Figure 10. Traceability for justification).

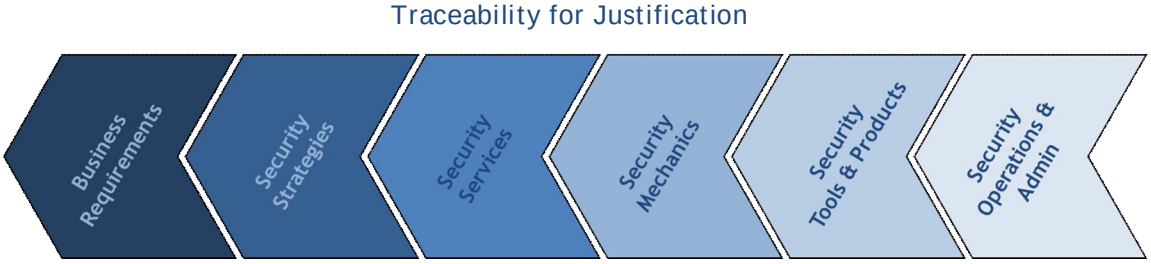


Figure 10. Traceability for justification (Sherwood et al 2005, 43&88)

5.4 Rules for the Documentation Framework

The efficient and easy to use structured documentation framework demands that the current documentation for a particular situation or type of work is easily found. The set of the current rules that effects or steers a certain situation or a role should be easily compiled. This requires that the documentation itself, its' content and naming as well as its information labeling has to be set up according to strict rules which benefits the ability to find the correct information.

5.4.1 Document Naming

Document naming and numbering needs to express the hierarchy in which the specific document belongs to. The name need also to express where the document inherits some of its features and is linking to. The naming and identification of specific documents as well as the search for certain documents in a document management system requires a strict naming structure.

Therefore, the Itella security policy framework will need clear definitions for document naming conventions even though the Itella organizational structure brings some difficulties to the taxonomy. The personnel need to have an understanding of the use of each type of document. The document naming convention, document text and its metadata together should describe to an individual these issues. The document name also has to amplify which organization has issued the document.

I would recommend the Itella document naming taxonomy to be a combination of Johnson's recommendation and change it to follow some of CERN's project specific naming structure. Also development ideas from a brainstorming session within Itella are included in the recommendation. Doing the combination of the naming structure based on the proposal is as it is seen on the figure (Figure 11. Naming structure example) and on the table (Table 2. Opening the naming structure) below. (Johnson 2011, 157 onward & (CERN 2011, 7).

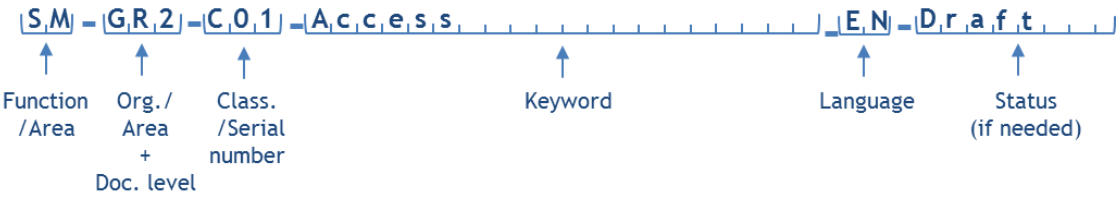


Figure 11. Naming structure example

The guiding principle in the naming structure proposal is that the search for the document in a system should be instinctive and help with searching for a document. The beginning of the name structure will directly limit the search to documents of a certain area and level. The use of a keyword also makes it possible to search certain topic area if the issuing function is not clear or the user cannot somehow determine that.

Function / Area	Organization identifier	Level of document	Classification	Serial nbr	Keyword	Language	Status (if not valid)
e.g. SM = Security Management	GR = Group CO = Corporation LO = Logistics MA = Mail Communications IN = Information	0 = Charter 1 = Policy 2 = Principle 3 = Standard 4 = Procedure 5 = Guideline 6 = Instruction	P = Public I = Internal C = Confidential S = Secret	e.g. 01	e.g. Access	EN = English FI = Finnish RU = Russian Etc.	(Empty) Draft Obsolete Expired
2 upper case characters	2 upper case characters	1 digit	1 upper case character	2 digits	Max 20 characters	2 upper case characters	Empty or 3 word choices

Table 2. Opening the naming structure

The Itella documentation hierarchy example below (Figure 12.) shows an example of a policy structure implemented in the policy hierarchy and its naming standard. There are five layers of documentation and the layers are:

- Security Charter
- Security Policy
- Information Security Principle
- Access Control Standard, Password Management Procedure and Authorizing Guideline
- Password Management Instructions

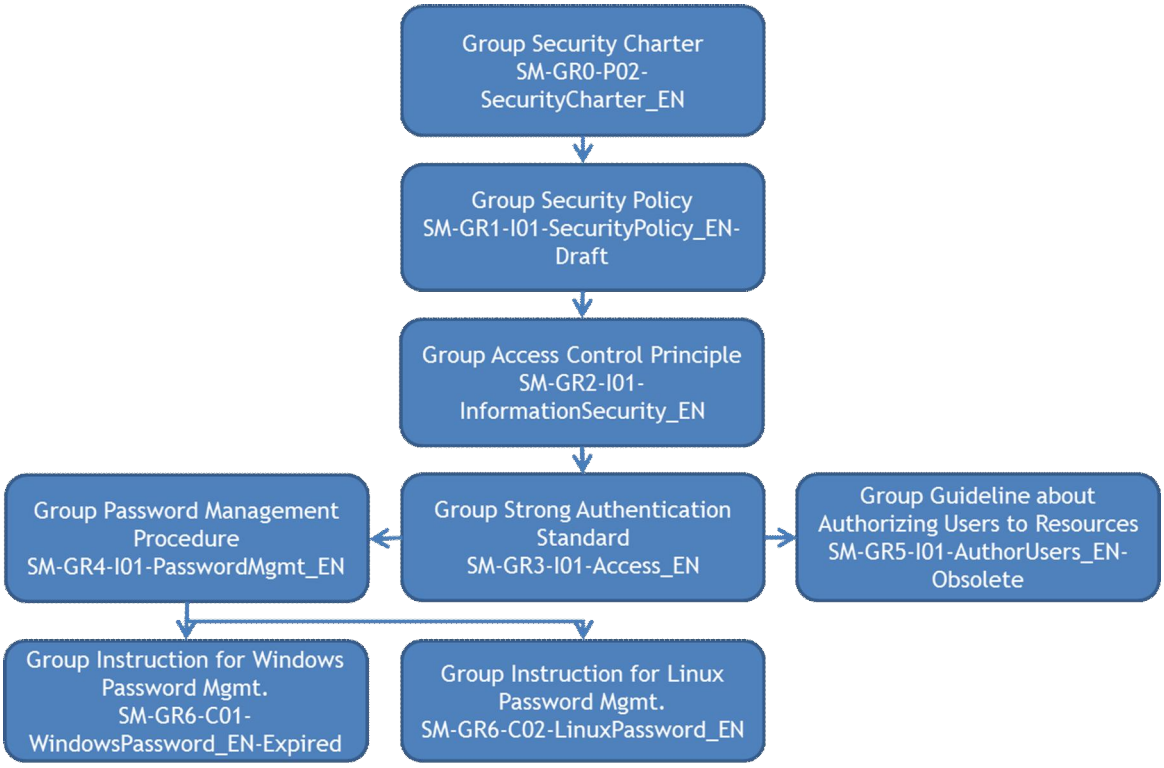


Figure 12. Itella documentation hierarchy example

The example (Figure 12.) gives a view about the policy framework in a case example where Itella level security charter and security policy are starting point for the structure. Beneath the policy, there is an access control related set of documents in a framework which is proposed to Itella. Also, the naming structure from the above table (Table 2.) is included to give more demonstrative picture about its usage.

5.4.2 Document Ownership and Approval

A successful policy framework needs a policy management and ownership model which helps the organization to see where the different level documents should get their approval from and which organizational level can own the different documents. Figure (Figure 13. Proposal for document ownership and approval) below shows the proposed document ownership and approval structure for Itella.

Without an ownership and approval model the documentation structure will become inconsistent and starts to contain duplications in the texts or at least in the efforts made for the documents. Clear ownership and approval model drives accountability and makes it easier to find the right party to contact if someone detects a clear need to update the document. Owner is also the one responsible of beginning the review and update process for the owned documents.

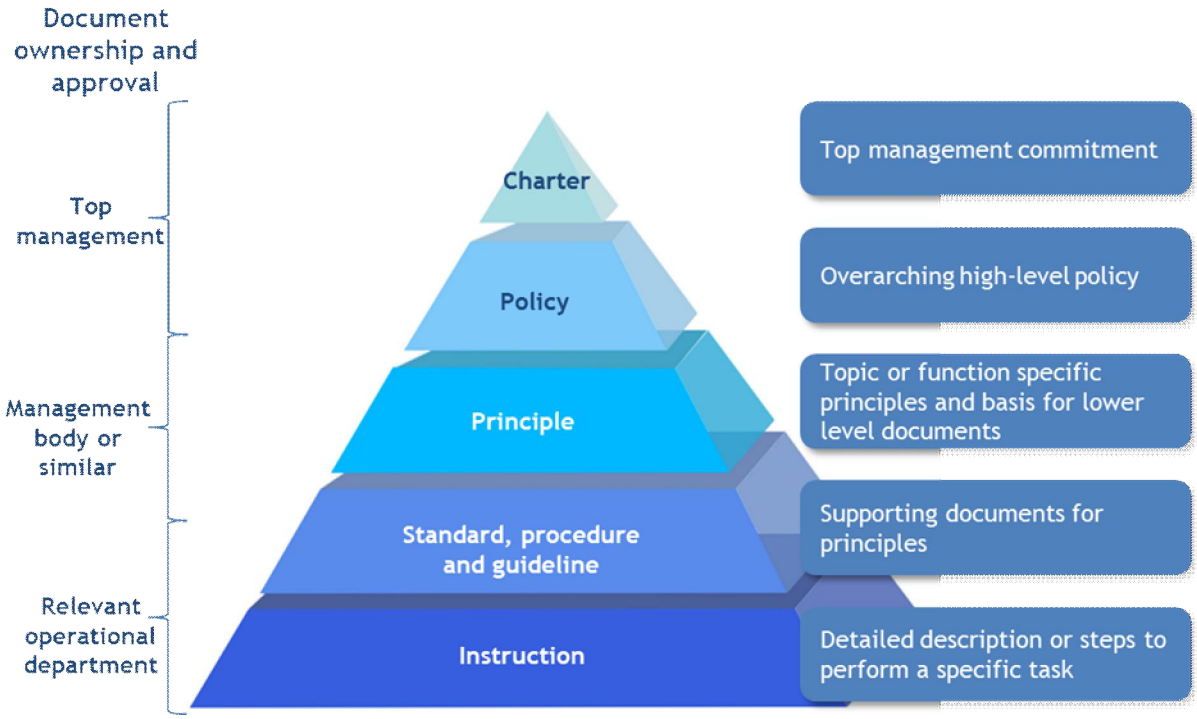


Figure 13. Proposal for document ownership and approval

The Charter which is the base of the security arrangements and contains strategic directives should be formed and owned by the CEO of Itella. The Business Group CEO's may issue their own Charter further defining and guiding the structures within their respective organization. Some of the Charter related directives have also been issued in the Itella Code of Conduct set of rules.

Policies dictate the organization responsibilities and mandates of different bodies within Itella. These should be owned and approved by the board of top management. The approving level has to have ownership, dictating power and mandate to the area and

Principles and standards should be owned and approved by the respective management team, security committee or similar bodies which have power to do so. Depending on the procedures and guidelines they go to the same category as principles and standards, but their approval and/or ownership can be given also to relevant operational department where at least instructions are owned and approved.

5.5 Document Lifecycle

Following chapters are handling some of the vital parts which should be part of the policy document framework and its handling in Itella. These have to be thought about and included before starting to implement the framework and put part of the guidelines for the framework usage.

5.5.1 Development

Several issues need to be considered, when the new governing documentation is made or the old one is updated. First of all, the need for the documentation and the type of internal regulation, and pros and cons must be weighed when answering the question "is the documentation at all needed"?

There are also external factors which must be considered when creating security documentation in different hierarchical levels (see chapter 3.4.1 and figure 4., page 29). Documentation may overlook some key issues without this knowledge. In higher level documentation issues such as organizations strategies have more effect for the document contents. Technological realities, chosen applications and implementation issues may influence more when developing lower level documentation. The document has to be the result of a thorough developing process where needs and requirements are detected and the document fulfills the needs and expectations put on it.

Also, a thorough risk analysis involving both the current situation as well as the future situation has to be made. This analysis may also be presented with several alternatives of different kinds of solutions for statements and controls.

The risk analysis has to consider the cost of implementation and life cycle management needed for the statement or control to be fulfilled. If the change from the current implementation is not mandatory based on external regulation or significant demand, at least the long term benefits must be higher than the costs of it. Therefore, both short and a long term impact analysis should be made.

The policy is approved and issued for use based on a decision made by the specific internal authority, a group or a person. To guarantee similar rigorous analysis will be made, the authority has to be the only one which can accept exceptions to the decided statements or controls.

When a new directing documentation is issued or relevant changes have been made to an old one, the implementation should contain a transition period or due time for compliance and adaptation for current implementations. All new implementations are expected to follow the new rules, if they are current when the implementation occurs.

5.5.2 Version Control and Document Metadata

Documents should always provide revision history, so that users can see what changes have been made to the document and also determine if they are looking at the correct version. (Fitzgerald 2012, 142). This can be done partly with the proposed document naming structure and partly with the version control and metadata.

Version control is a necessary part of document management. Personnel have to be aware of such things as which document is currently effective. Also, if the document replaces an earlier document or the document has been replaced by another should be known from the document.

Document metadata can be used for many things. There can be a document metadata which is in the document properties and also a metadata in the document text itself.

Documents need to contain metadata also about their approval level, ownership, period of validity, etc. The document can contain many metadata fields and table below (Table 3. Documents internal metadata example) serves as an example of that in Itella.

Approved	**At:**	**By:**
Prepared		**By:**
Effective	**From:**	**To:**
Obsoletes	**List of documents**	
Obsoleted by:	**List of documents**	
Review	**Yearly. (max 18 full months)**	**By:**

Table 3. Documents internal metadata example

Brotby (2009, 116) stated that policy needs as many standards underneath it as there are classification levels in the organization. In Itella there are commonly four levels of classification; public, internal, confidential and secret. If Itella would start to write standards for every classification level the document architecture would expand and the understanding of the structure might decrease and finding the needed information would be difficult.

Since some of the standards will likely contain different directives or controls to the different classification levels, they should have a notations practice to differentiate the directives per classification level when needed. This is built inside the document text per issue to control. Mainly this would mean that the standards would have different set of directives or control types for different classification levels. The level specific directives should be marked clearly. This should be done in the document per objective in such way that it is possible and easy to find the information while reading the document.

A clear and simple way of telling which parts of the document applies to which classification level should be more sufficient. An example could be to use a table like the one below (table 4. Proposal for differentiating requirements per classification level).

ID	Public 1-3	Internal 1-6	Confidential 1-3, 6, 8	Secret 1-3, 7-10

Table 4. Proposal for differentiating requirements per classification level within the document (NIST 800-53).

The standard could be containing for example 1-10 different directives, rules or controls to be followed amongst the other subject areas. The table within the document would tell that if confidential material is handled the directives 1-3 and also 6 and 8 have to be applied. Directives 4-5, 7 and 9-10 would not apply in that case.

I recommend Itella to get to know National Institute of Standards and Technology special publications 800-53 type of notation when differentiating classification related controls. (NIST 800-53).

5.5.3 Publication

Even the best governing documentation is useless if no one knows about it. Therefore the publication and way of doing it as well as the way how the document is saved and kept available for the ones needing it is so important.

The publication of a new document should at least be done so that those who have to implement the new ruling are aware of its existence. This would mean a campaign and possible education to be organized. This would also in some cases need to involve communications specialists to do a plan for issuing a new regulation.

The storing of and possibility to search for a document is an important factor. The document metadata as well as the naming of it plays a crucial role. Also, good referencing ("links") between the different documents needs to be built to get the full relevant set of documentation.

5.5.4 Follow-up Process

The follow up of a regulative document is important. After a certain time after issuing a document it is expected to be implemented everywhere that it applies. This transition period should be said in the document itself.

After the transition time has expired, all the situations where the documentation and the rules in them are not followed are to be handled as breaches of security. What the actual consequences of such are depends very much on the organization. There should be a method applied to enforce the application of the documents and their rules. For many companies the only method is escalation, which in some cases is not effective, if the management does not react on the nonconformance. Then this is not valid either.

The actual follow-up of compliance is done in internal audits and in inspections made to different parts of the organization. Sometimes even external audits may reveal nonconformance with the standing documentation. Anyway, if such is found, an exception process needs to be started immediately in cases where it may apply. In other cases the change for a compliant implementation has to be done immediately.

5.5.5 Exception Handling

Risk management as well as all new development made relies on the assumption that the defined processes and working environment have been implemented as designed. This baseline is formed by the guiding documentation. It presents the measures taken within and controls defined to the area and scope of the policy document.

If uncontrolled exceptions to the baseline are made, there is no possibility to control the behavior of the environment. All the policy documentation containing controls and methodologies are made after assessment of cost and risk involved for chosen controls and statements. A non-standardized implementation may add vulnerabilities and cost to the organization and its environment. A non-standardized environment can also lead to a situation where the risk management as well as development initiatives lack important cornerstone.

Itella, its Business Groups and units must follow the Itella baseline and comply with it. If some function is not using for example technology which is capable of complying with the mandatory principles and standards they are not free from responsibility. They must alternatively present security controls and standards in a documented manner. Also, alternative solutions must be able to be audited against agreed alternative standards. Normally exceptions must be for a temporary fixed-term period only. All exceptions have to be documented and agreed-upon.

Johnson presents, that when the exception process is implemented the following should be considered:

- "Independence – Be independent of the business unit seeking approval.
- Impact – Examine the risk to the entire organization.
- Benefits – Understand the business benefits.
- Mitigation – Identify security controls outside policy.
- Approvals – Residual risk should be formally accepted by management". (2011, 41).

This is a very good summary of things to consider. Johnson though looks only at the implementation side of the issue. He should also add the cost and risk management view to this to get more complete picture.

The one owning and issuing the rules is the only one to accept an exception application. Handling power of exceptions approval may be delegated to be fully or partly handled by another position or a specific part of the organization.

5.5.6 Document management policy

Since the policy framework document hierarchy and formulation of it will have many rules and guidelines to follow, I would recommend Itella to have a policy formulation and handling guidelines. Those guidelines are also called for a policy of policies or metapolicy. This policy would inform the organization on how policies should be created, implemented and enforced in order to assure that all policy related documents in the organization are aligned correctly, contain the right level of information, and will be kept up-to-date. Changes to the documents are inevitable for example due to organizational or strategy changes. Policies and related documentation should then also be changeable and metapolicy should contain guidelines for doing that, allowing rapid reaction for change when it is needed. (Baskerville & Siponen 2002, 338).

The document management policy should be answering questions like: who establishes policy and is accountable and the owner of it, who is accountable for its updates and how often the

documents should be reviewed, what exactly constitutes a policy, how will it be stored and for how long, as well as how the versions will be handled. The same kind of questions should also be answered according to other level documents in the policy framework and their management. The policy of policies should also tell which documents are mandatory to follow and which ones are recommendations.

The document management policy would also be the right place to lay down rules such as which language version of the documents is the main version. Itella common language is English and it should be the official language for the documents in the documentation framework. In case of language version misalignment, the Intranet English version would always apply officially.

6 Tabletop Testing the Framework Implementation

The usability and impact of the security policy framework can only be seen after the implementation and use of it for a long period of time. It can also be seen from possible cultural changes which will be forming after the implementation. Actual implementation of the security document framework in a real life environment is out of the scope of this thesis. The framework will be implemented in Itella, but it was not possible to do that in the timeframe where those experiences could have been included in this thesis.

Instead, the framework has been tested with various real life scenarios within Itella. This process is described in the next chapter. The testing has been done with the security policy framework which can be seen at the Figure 8. (The security documentation framework proposal for Itella) in the page 47.

6.1 Case Study in Itella

At this point the evaluation of the framework was done as an action research project consisting several workshop sessions (Appendix 2). The proposed structure for documents was tested in workshops together with professionals from Itella.

Each testing session started with a drawing of the basic structure where Charter, Policy, Principle, Guideline, Standard, Procedure and Instruction were in a hierarchical order. Organized brainstorming sessions were held having different main topics per session. During them, several scenario based cases were tested. Testing was done mainly so that a specific topic was discussed and the case was gone through with the structure thinking what kind of documents could be needed to direct and guide the process through.

In Appendix 3 one of these sessions is presented. The leading topic in this case was a new employee starting to work for Itella. Those documents are marked with blue background which was seen in this case as the ones needed to guide the example process through.

On Charter and Policy level the manager of the person is given the responsibility to take care of the induction period of the new recruit. This also contains the requirement to supply her with tools and the access rights needed for the intended work as well as the initial training in security.

The manager applies for access to premises and systems. The principles of the access rights are given and fulfilled with the procedures for doing the concrete work for granting the rights. The person will also get an account, which is created using certain standard settings.

The user account will be added as a member in groups giving her access, membership in mail lists etc. When the user gets the account, she has to create herself her own authentication password. This has to be according to that particular standard.

The above scenario is well defined in the tabletop tests. The tests show the importance to use the levels correctly. For instance, a general instruction can be referred to from the other documents. The method seems to resemble the way a computer program is built, by calling procedures and functions from different places and to use the same common parts in several places. This also has an impact on how the documentation set can be managed. For example in the tabletop test (Appendix 3) human resources and security documentation can be referenced between each other's.

Examples of the other bigger tabletop test exercise scenarios which were done are included in the following scenario list:

- Employee leaving Itella
- External consultant on boarding and off boarding
- Itella Information's current information security documentation including a new addition of a security committee as part of the organization governance model
- Handling of customer data
- Audit procedure
- Risks management in a project framework

As a compliment and part of these scenarios also smaller tests were done and discussed about. These included particular issues such as making and handling of system and data backups, information classification and handling, email and internet usage.

The above procedures and the documentation linked to them were able to be put in a logical way into the structure proposed.

7 Value and limits of the study

Kasanen et al (1993, 253) defines that the usefulness of a construction can be proven only after practical testing has been done and the construction has passed the tests. The subject of this thesis narrows down the possibilities to test the construction. Full testing will happen when the current documentation will be transformed to the new framework and it is applied to new documents.

It is still obvious that different parties will benefit from this work and the work done when utilizing the proposals in this study. All the benefits and also drawbacks can be seen after the implementation of the framework.

7.1 Value to Itella

The presented structure will help in reorganizing the whole governing documentation in security. This will hopefully lead to a better utilization of the current ruling in the whole Itella as well as easier maintenance of them. The structure and related points in this thesis should be able to raise awareness about the documentation, make it easier to access and getting it to be more up-to-date.

The documentation structure will be presented to Itella's Corporate Security and taken into use as soon as it is finalized and tested successfully for existing security documentation. The ideas of this thesis have been already used on some new documents but the old documentation will not be started to transform before going the structure through with the Corporate Security function.

This study has emphasized the framework for documents within security since the author is a security professional and the thesis is done for the security competence programme. During the whole development procedure there has also been a hidden agenda involved. This is to develop the hierarchy and document types so that they can benefit other areas and functions in Itella. The created framework fulfils that need and may be directly applied to other types of guiding documentation. The framework may even be a starting point for a common documentation structure in Itella. The presentation about the structure will be made to Itella Strategy Director when the thesis has been finalized. After that we will see if there is a possibility to grow to the common structure.

It has already been seen in Itella after the recent CEO change that the mandate to approve has to be delegated to lower levels from the executive level. Earlier EB/MB has approved policies including quite low-level content. It is a clear signal to delegate mandate for lower level

issues when Management/Executive Board starts to meet less frequently. To me this seems to be a good moment to also push a new structure into use in the organization. This is a clear sign of the desire and intent to streamline the meetings and taking only the correct level issues to the agenda.

7.2 Value to the customers

When the security documentation is in a well-structured form it is easier to present to the customers when needed. It will show an example of a well-balanced security management system. When the personnel in different roles can find the security documentation and are aware of its existence they are able to act according to those laid rules. All this would also help in streamlining possible customer audits when the documentation can be found and the customer focus on assessing the actual processes via examples. This would be a great means to build trust between Itella and its customers.

7.3 Value to other organizations

Several individuals from other organizations have shown their interest towards this work already before it has been completed.

As seen in the study, it seems that although organizations have not noticed that their structure of documents is defective in any way, they suggest in many cases another way of organizing the documentation. The way presented here could very well solve other organizations challenges. During the interviews one interviewee even told me that they are moving towards a system that resembles almost one to my suggestion. This is interesting since they have come to the same conclusion even though it is not like anything implemented in any of the companies answering my questionnaire.

The ideas tested and presented on those who have contacted me have been received very well. As this is not anything that has been much studied before, we might see some changes in how companies see their documentation structured. I have presented one structure, but I expect more studies to come up with new thoughts.

I don't expect this set of documentation to conquer the whole world, even though it may via Finnish companies and the security persons own networks spread and I think at least that will be given a thought and a consideration.

7.4 Limits of the study

The main limitation for this study was the fact that security documentation framework is a topic which has not been researched. There are no researched outcomes which would prove one framework better than the other. There are no outcomes which would tell which kind of framework would be easiest to maintain, better understood by the personnel or if the framework affect all this. It is unknown what constitutes an effective security policy framework if research is concerned. Also, organizations business environments and the culture vary which most likely lead to a situation where there is no one framework which fits to all. When corporate culture is formal, the policy documentation should be more defined with clear boundaries and if the culture is informal the same legalisms might not work.

Many organizations have gotten used to the document set they have, and do not put many thoughts into the fact that it might be hard to maintain or if it is optimal for their use. Therefore, if they do not see the situation or the problem itself, then it may also put an angle on the answers I have received. Still, my questionnaire shows that they are not fully satisfied with their current situation.

8 Conclusions

I have in this study, as soon as I found it out, walked on uncharted territory. I had to build my idea based on the few documents and also literature covering something about the topic and some ideas built from my peers in other organizations, as well as testing the result with some experts and on our settings. Scholarly studies are not available about this topic area.

My goal to build a security policy framework that would suit at least the needs of Itella has, based on the organization's responses, been successful. The idea for the structure will be taken into use and implemented starting by having a security charter written by the CEO. In tests, the structure has proven to be easily understood, even though there is some need to put effort in describing and teaching the meaning of the levels for the policy developers. This is manageable and will, according to comments, at least be clearer than the situation is today. I will also be presenting the framework for the Itella Strategy Director who is already interested in knowing would this framework work as a common documentation structure for Itella. The security framework proposal is going to be proposed to transform to the common documentation structure for Itella.

The created framework showed both traceability of the rules, but also a justification for implementation may be seen to exist. This comes true to the extent the documentation structure can facilitate the idea. The justification is a bit harder to be clearly determined in a real case situation.

The documentation naming structure, which was created during the study with flavors borrowed from CERN and Johnson, seems to be suitable for the need of Itella. Parts of traceability to both ways can be verified from the naming, and it also states the classification information and many structure parts which can be used for searching documents.

All in all, I see this study as having been successful in all the goals set. Itella will now have a new set of material which can form the structure of its security architecture as well as its documentation.

Once again I want to give my greatest thanks to all the individuals in different organizations that have given their input for my study. This would not have been a success without them.

8.1 Future Research

The development of the security policy architecture in Itella will continue based on the developed policy framework. It is a long-term project to form comprehensive security policy architecture, and it will take time to see how well the policy framework is working and will it be implemented to documentation as a whole.

So the usability and impact of the policy framework can only be seen after the implementation and using of it for a longer period of time. It will also be influenced by the culture which will be forming after the implementation. Only then will we see if the framework is helping to understand the differences in document types and if the organization is able to keep the documentation as a whole more organized and maintained.

As this topic within research seems to be a new and uncharted area, further studying, and maybe general standardization would be a good way to go forward. I see that this topic could also form a new standard into the ISO set of standards as this is still missing. This way a good practice would more quickly become a norm. This would also help implementation and understanding of the whole structure over organizational borders.

A topic to continue studying is the maintenance and management part as well as the publication of the structured documents. The first interesting area for research is reviewing and keeping the documentation up-to-date. Can the structured document format with decentralized issuing of norms be more easily maintained? The latter part, publication, could be a usability study for instance on how the structured setting would help to create a dynamic handbook of rules for different roles in an organization.

Another area of interest for study would be monitoring the document system and making metrics on how the structure influences on behavior of the workforce as well as comprehension of the whole set of rules. Also getting an answer for the following questions would be interesting. Can the structure make it easier to be compliant? Will it help to find the correct set and implement it as desired?

References

BOOKS AND PUBLICATIONS

Bacik, Sandy 2008. Building an Effective Information Security Policy Architecture. CRC Press LLC. Boca Ranton, Florida, United States of America.

Cannon, David L. 2011. CISA: Certified Information Systems Auditor study guide, Third Edition. Wiley Publishing, Inc., Indiana, United States of America.

Fitzgerald, Todd. 2012. Information Security Governance Simplified. From the Boardroom to the Keyboard. CSC Press, Taylor & Francis Group, LLC.

Itella Corporation. 2012. Annual and corporate responsibility report 2011. Erweko Oy.

Johnson, Rob 2011. Security Policies and Implementation Issues. Jones & Bartlett Learning LLC. United States of America.

Kasanen, Eero & Lukka, Kari & Siitonen, Arto 1993. The Constructive Approach in Management Accounting Research. JMAR, Volume Five, Fall 1993.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät: uudenlaista osaamista liiketoimintaan. WSOYpro Oy, Helsinki.

Peltier, Thomas R. 2004. Information Security Policies and Procedures: a practitioner's reference. 2nd edition. CRC Press LLC. Boca Ranton, Florida, United States of America.

Peters, Michael D. 2012. The Holistic Operational Readiness Security Evaluation: HORSE Project Series Volume 1. Governance Documentation and Information Technology Security Policies Demystified. Amazon Distribution GmbH, Leipzig, Germany.

Puhakainen, P., Siponen M., Karjalainen M. 2010. The Dewald Roode Information Security Workshop, IFIP WG 8.11/11.13, 2010. http://ifip.byu.edu/ifip2010.html

Sherwood, John & Clark, Andrew & Lynas, David 2005. Enterprise Security Architecture: A Business-Driven Approach. CMP Books. United States of America.

Wahe, Stefan 2011. Open Enterprise Security Architecture (O-ESA) – A Framework and Template for Policy-Driven Security. The Open Group. Van Haren Publishing.

ELECTRONIC REFERENCES

Allen, Julia 2007. Governing for Enterprise Security (GES) Implementation Guide. Referred 27.1.2013. http://www.cert.org/archive/pdf/07tn020.pdf

The American Heritage dictionary of the English Language. Houghton Mifflin Harcourt Publishing Company. Referred 23.9.2012.
http://www.ahdictionary.com/

Baskerville, Richard & Siponen, Mikko 2002. An information security meta-policy for emergent Organizations. Referred 8.1.2013.
http://www.tol.oulu.fi/projektit/fusion/public/2002%20An%20Information%20Security%20Meta-policy%20for%20Emergent%20Organizations.pdf

CERN 2011. Document types and naming conventions. The Large Hadron Collider project. Referred 20.2.2013.
http://lhc-proj-qawg.web.cern.ch/lhc-proj-qawg/CD-ROM/Quality/QA202.pdf

Corporate Governance Task Force 2004. Information Security Governance: A Call to Action. Referred 15.1.2013.
http://www.cyber.st.dhs.gov/docs/Information%20Security%20Governance-%20A%20Call%20to%20Action%20(2004).pdf

Itella 2012a. Company information. Referred 17.9.2012.
http://www.itella.com/about/companyinformation.html

Itella 2012b. Business areas. Referred 17.9.2012.
http://www.itella.com/businessareas/

Itella 2012c. About Itella Group, Referred 14.10.2012.
http://www.itella.com/about/media/faq/aboutgroup.html

Itella 2013a. Group Companies. Referred 17.3.2013.
http://www.itella.com/about/company/organization/groupcompanies.html

Itella 2013b. Itella takes responsibility openly and reliably. Referred 4.2.2013
http://itella.com/about/responsibility/

Johansson, Erik & Ekstedt, Mathias & Johnson, Pontus 2006. Assessment of Enterprise Information Security – The Importance of Information Search Cost. Proceedings of the 39th Hawaii International Conference on Systems Sciences 2006. Referred 4.3.2013.
http://origin-www-ca.computer.org/csdl/proceedings/hicss/2006/2507/09/250790219a.pdf

Nielsen, Jakob 1994. Jakob Nielsen's Alertbox: January 1, 1995. 10 Usability Heuristics for User Interface Design. Referred 14.4.2013.
http://www.nngroup.com/articles/ten-usability-heuristics/

Nielsen, Jakob, Molich, Rolf 1990. Heuristic evaluation of user interfaces. In proceedings of ACM SIGCHI. Referred 14.4.2013.
http://doi.acm.org/10.1145/97243.97281

NIST 800-53, Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology, Special Publication 800-53. Referred 3.2.2013.
http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800_53_r4_draft_fpd.pdf

Rasmussen, Michael 2012. Why Do Policies Matter? Referred 20.1.2013.
http://www.complianceweek.com/why-do-policies-matter/article/247816/

Charts

Figures

Tables

Appendices

Appendix 1 Questionnaire for Security Experts about Security Policy Architecture (In Finnish)

Kyselytutkimus turvallisuusdokumentaatiokokonaisuuteen liittyen

Johanna Kinnarin tekeillä olevaan opinnäytetyöhön liittyvä kysely. Kysely on suomenkielinen, mutta itse opinnäytetyö on englanninkielinen. Opinnäytetyö liittyy opintoihin turvallisuusosaamisen koulutusohjelmassa (tradenomi ylempi AMK, Laurea).
* Required

Oheisessa kyselyn ensimmäisessä osuudessa sinun tulee vastata kysymyksiin oman organisaatiosi olemassa olevan turvallisuusdokumentaation kannalta

Kyselyssä olen luetellut dokumenttityyppejä englanniksi, mutta mikäli teillä on käytössä vastaavia tyyppisiä muilla kielillä, niin lähin vastaava valitaan.

Mitä turvallisuuteen liittyviä dokumenttityyppejä organisaatiossanne on käytössä ja mikä on (jos on) niille määritelty hierarkia? *
Valitse yksi per rivi.

	Top - 1.	2.	3.	4.	5.	6.	Ei määriteltyä hierarkista sijaintia	Ei käytössä organisaatiossamme
Baseline	○	○	○	○	○	○	○	○
Charter	○	○	○	○	○	○	○	○
Guideline	○	○	○	○	○	○	○	○
Instruction	○	○	○	○	○	○	○	○
Policy	○	○	○	○	○	○	○	○
Procedure	○	○	○	○	○	○	○	○
Standard	○	○	○	○	○	○	○	○

Mikäli teillä on käytössä muita dokumenttityyppejä, pyydän listaamaan ne oheen.
Voi olla myös suomenkielinen nimitys. Lisää myös yllä olevan taulukon mukainen hierarkian järjestysnumero, mikäli sellainen on määriteltävissä. Voit halutessasi lisätä myös selventäviä kommentteja.

Onko organisaatiossanne olemassa dokumenttia, joka ohjaa dokumenttien luontia, nimitystä, hierarkiaa ja hyväksyntää?
Kerro tällöin lyhyesti mitä ohjeistus pitää sisällään.

Continue »

Kyselytutkimus turvallisuusdokumentaatiokokonaisuuteen liittyen

* Required

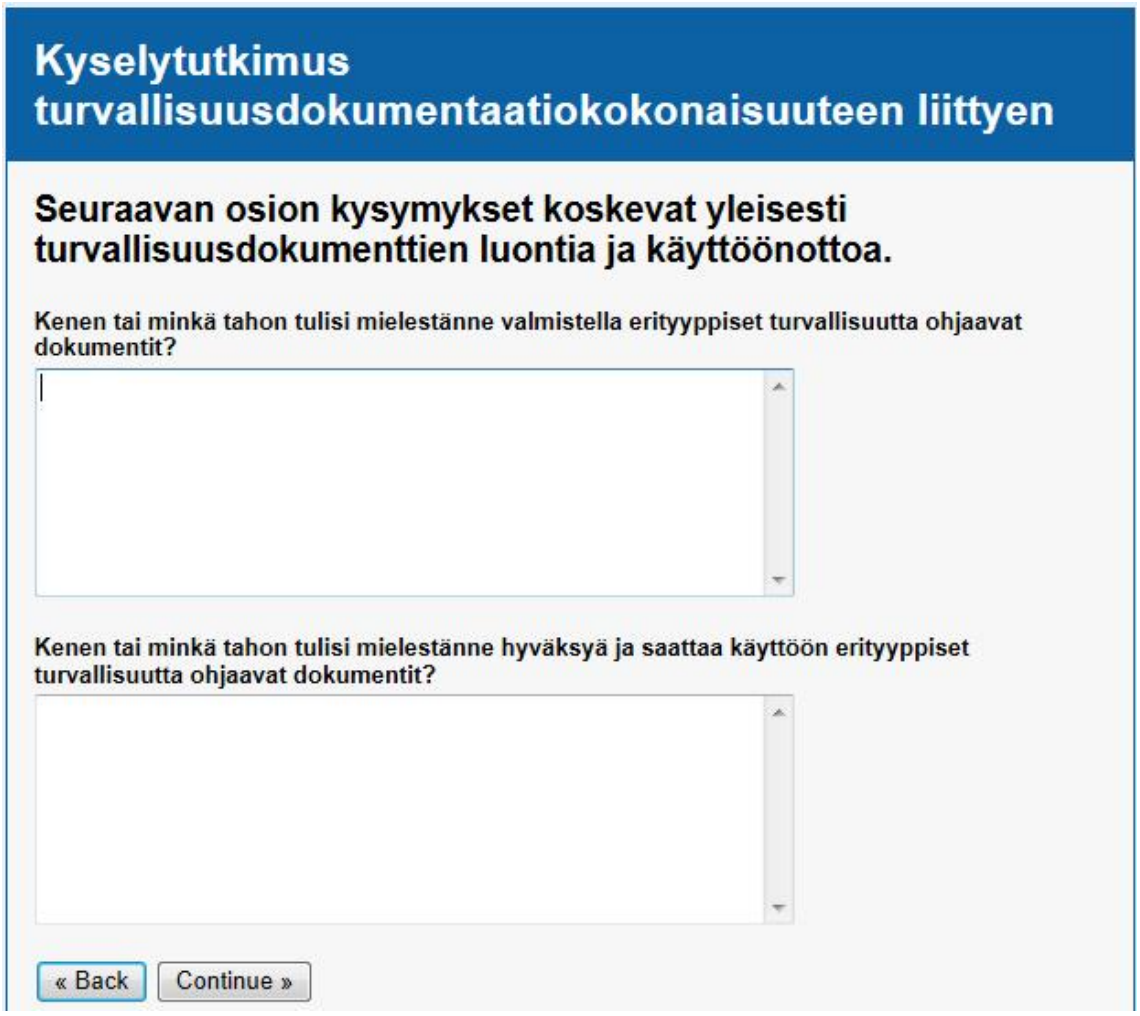
Seuraavassa osuudessa sinun tulee ajatella asiakokonaisuutta yleisemmin, ei oman organisaatiosi näkökulmasta.

Määrittele seuraavat dokumenttityypit mielestäsi loogiseen hierarkiseen järjestykseen. *

	Top - 1.	2.	3.	4.	5.	6.	En näe tätä tyyppiä tarpeellisena
Baseline	○	○	○	○	○	○	○
Charter	○	○	○	○	○	○	○
Guideline	○	○	○	○	○	○	○
Instruction	○	○	○	○	○	○	○
Policy	○	○	○	○	○	○	○
Procedure	○	○	○	○	○	○	○
Standard	○	○	○	○	○	○	○

Mikäli vaihtoehdosta puuttuu mielestäsi dokumenttityyppejä, pyydän listaamaan ne oheen tai mikäli haluat kommentoida edellistä, se on mahdollista tässä kohdassa.

« Back Continue »



Kyselytutkimus turvallisuusdokumentaatiokokonaisuuteen liittyen

Seuraavan osion kysymykset koskevat yleisesti turvallisuusdokumenttien luontia ja käyttöönottoa.

Kenen tai minkä tahon tulisi mielestänne valmistella erityyppiset turvallisuutta ohjaavat dokumentit?

Kenen tai minkä tahon tulisi mielestänne hyväksyä ja saattaa käyttöön erityyppiset turvallisuutta ohjaavat dokumentit?

« Back Continue »

Kyselytutkimus turvallisuusdokumentaatiokokonaisuuteen liittyen

* Required

Olen opinnäytetyössäni luomassa ehdotusta hierarkiajärjestelmästä turvallisuusdokumentaatiolle.

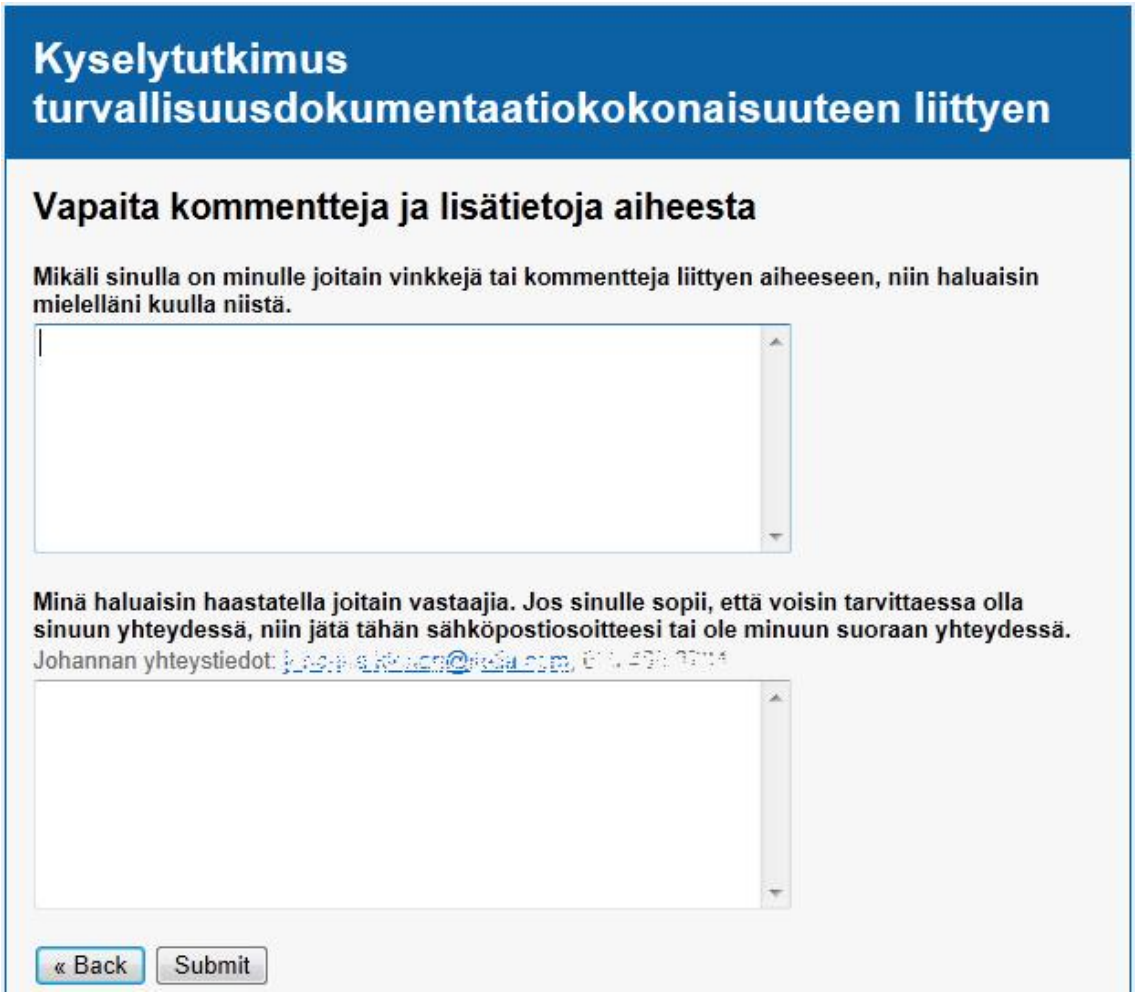
Haluaisin kuulla vapaata mielipidettäsi tällaisesta.

Minkälaisia tärkeimpiä ominaispiirteitä näet hyvän hierarkisen turvallisuusdokumenttirakenteen omaavan? *
Listaa ominaispiirteitä haluamasi määrä ja aloita sinulle tärkeimmästä ominaispiirteestä. Numeroi tarvittaessa (selkeyttää).

Minkälaisiin asioihin hierarkisella dokumenttirakenteella voisi olla positiivista vaikutusta?
Täsmennä vaikutuksia kuvailemalla

Minkälaisiin asioihin hierarkisella dokumenttirakenteella voisi olla negatiivista vaikutusta?
Täsmennä vaikutuksia kuvailemalla

« Back Continue »



Kyselytutkimus turvallisuusdokumentaatiokokonaisuuteen liittyen

Vapaita kommentteja ja lisätietoja aiheesta

Mikäli sinulla on minulle joitain vinkkejä tai kommentteja liittyen aiheeseen, niin haluaisin mielelläni kuulla niistä.

Minä haluaisin haastatella joitain vastaajia. Jos sinulle sopii, että voisin tarvittaessa olla sinuun yhteydessä, niin jätä tähän sähköpostiosoitteesi tai ole minuun suoraan yhteydessä.

Johannan yhteystiedot:

« Back Submit

Appendix 2 Timetable for Questionnaire, Evaluation Sessions, and Internal Workshops

Questionnaire

Sent during 28th February 2013 and closed at 14th March 2013

One-to-one evaluation sessions

1st evaluation interview
20th March 2013

2nd evaluation interview
22nd March 2013

3rd evaluation interview
27th March 2013

4th evaluation interview
27th March 2013

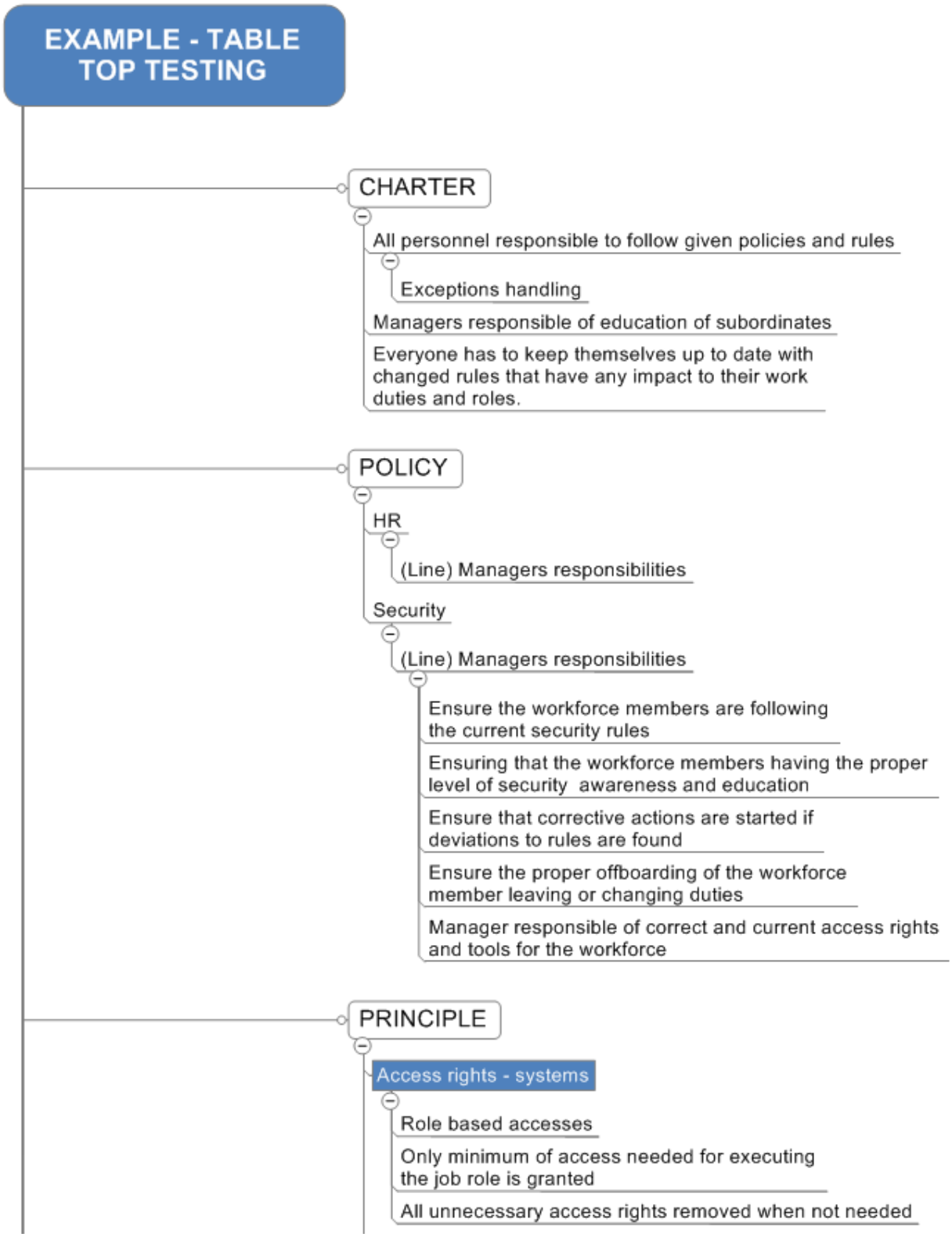
Internal workshops

1st session
20th March 2013

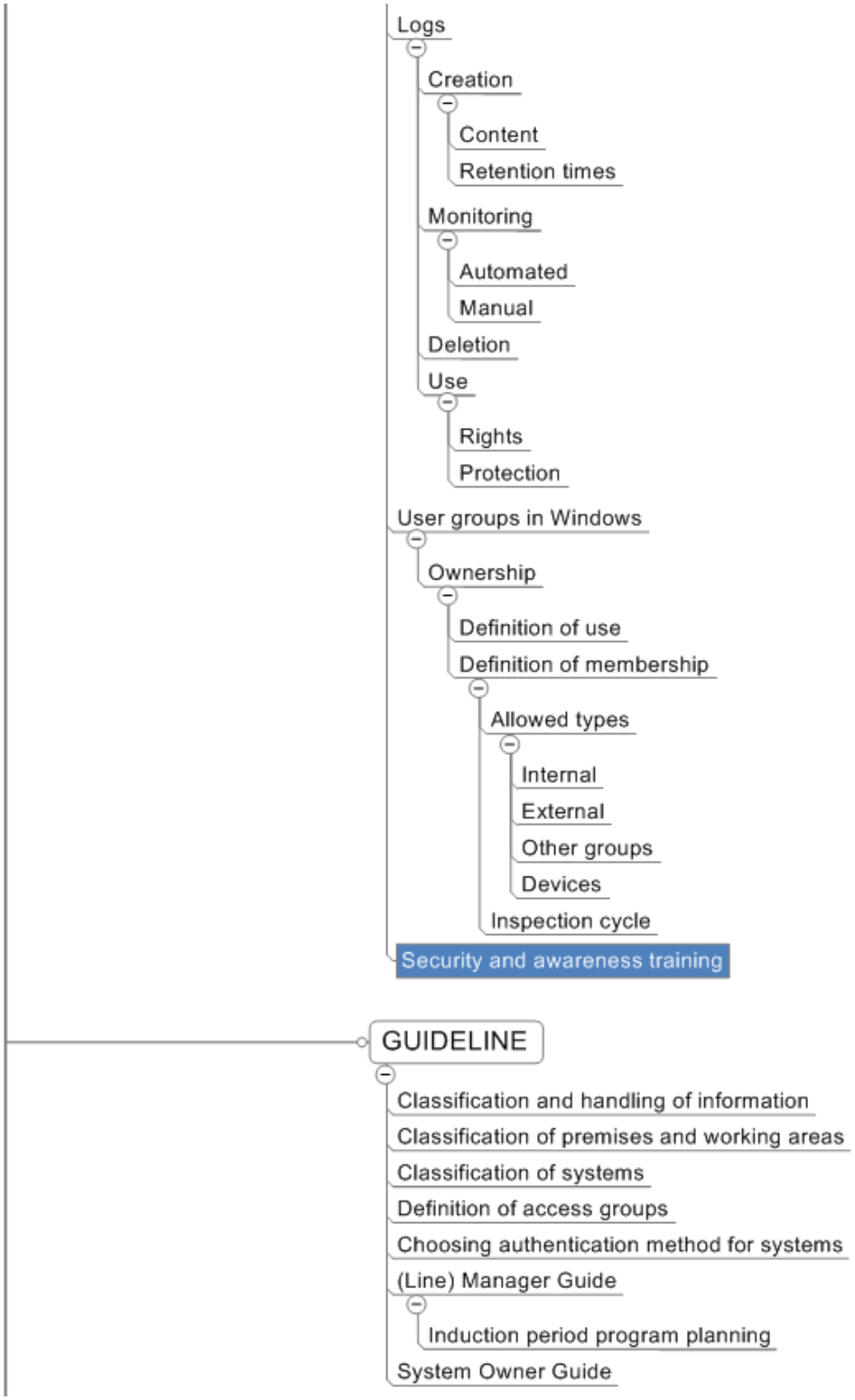
2nd session
22nd March 2013

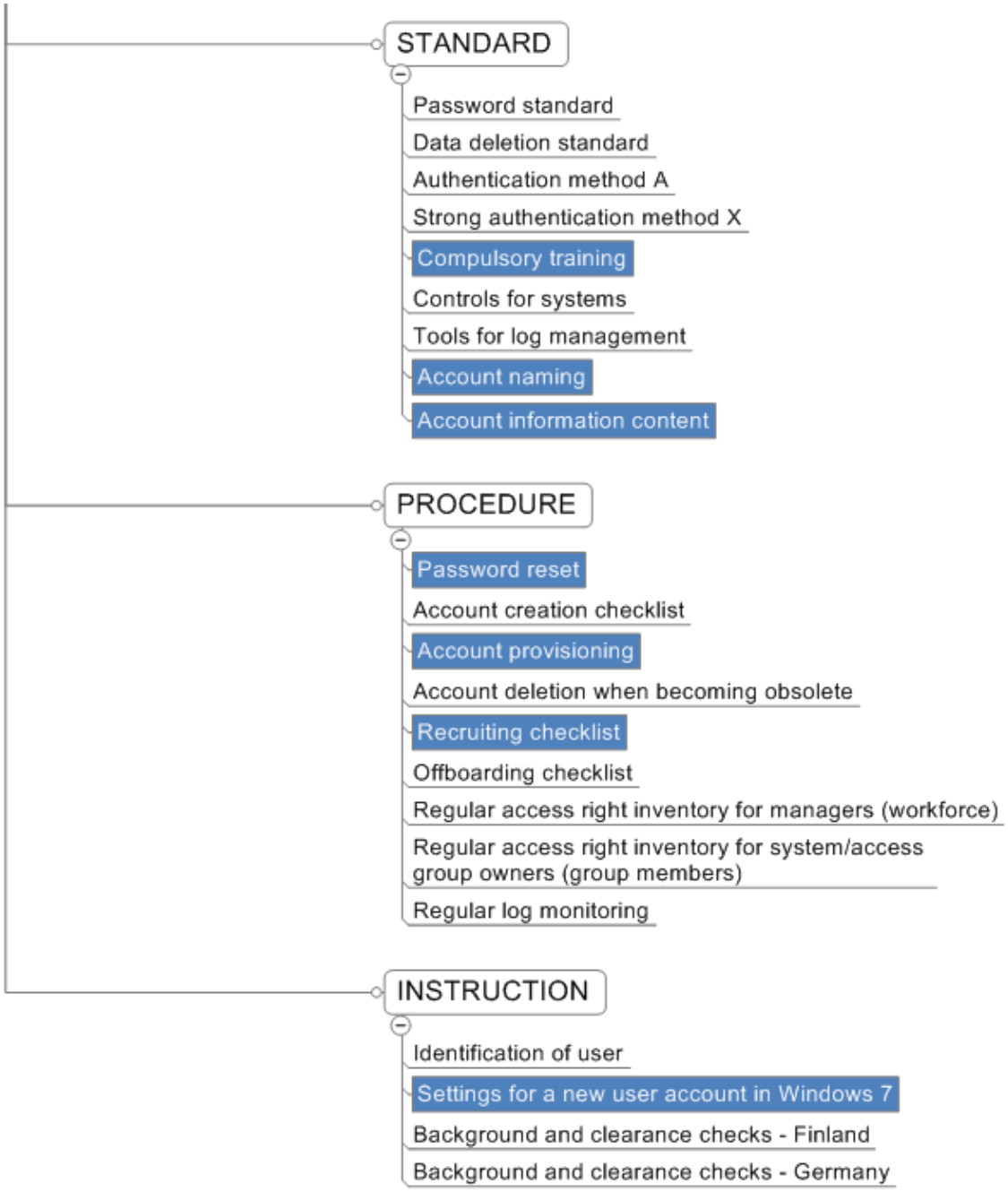
3rd session
27th March 2013

Appendix 3 Framework Implementation Case Study example




Access rights - premises
Role based accesses
Only minimum of access needed for executing the job role is granted
All unnecessary access rights removed when not needed
Electronic keys are to be used in all premises
Instructions for local access management has to be created
Accounts
Use may be logged
Lifecycle
Creation
Deletion
Types
Personal
Internal
External - partner
Local workstation administrator
Group account
System account
Support account
Administrator - server/system
Administrator - workstation
Authentication
Authentication when intranet used
Authentication from internet
Strong authentication
Personnel lifecycle
Recruiting
Initiation
Change of work
Leaving


Logs
Creation
Content
Retention times
Monitoring
Automated
Manual
Deletion
Use
Rights
Protection
User groups in Windows
Ownership
Definition of use
Definition of membership
Allowed types
Internal
External
Other groups
Devices
Inspection cycle
Security and awareness training
GUIDELINE
Classification and handling of information
Classification of premises and working areas
Classification of systems
Definition of access groups
Choosing authentication method for systems
(Line) Manager Guide
Induction period program planning
System Owner Guide


STANDARD
Password standard
Data deletion standard
Authentication method A
Strong authentication method X
Compulsory training
Controls for systems
Tools for log management
Account naming
Account information content
PROCEDURE
Password reset
Account creation checklist
Account provisioning
Account deletion when becoming obsolete
Recruiting checklist
Offboarding checklist
Regular access right inventory for managers (workforce)
Regular access right inventory for system/access group owners (group members)
Regular log monitoring
INSTRUCTION
Identification of user
Settings for a new user account in Windows 7
Background and clearance checks - Finland
Background and clearance checks - Germany