Controlling risks when integrating Mobility and Enterprise Resource Planning (ERP)

The development of a Mobile-ERP control framework (M-ERP CF)

"Organizations either do not adopt ERP mobility because they feel like it is not secure enough, or they do, but without realizing its impact and simply see where it goes from there"

Deloitte.

Universiteit Utrecht

Master thesis (Final)
February 22nd, 2015
Rodi Heijblom (3489787)
RHeijblom@deloitte.nl

Master of Business Informatics,
Utrecht University

Supervisors
Utrecht University:
Dr. F.J. Bex
Dr. M.R. Spruit

Deloitte Risk Services:
Ron Hakvoort

Abstract

The goal of this thesis was to investigate the impact of integrating mobile technology as an extension to existing and more traditional Enterprise Resource Planning (ERP) systems. A process was initiated to identify new risks that arise from the integration between back-end system and mobile device, and also to evaluate existing risks that might be altered or amplified due to mobility. Subsequently, controls were defined that cover the threat landscape and risks relevant to a M-ERP solution. Together, these two components (risks and controls) compose the essential elements for the main artifact developed in this thesis: a control framework that can be used to gain insight in the risks involved with ERP mobility as well as ways to mitigate those risks. The framework can be used by (IT) auditors in their day-to-day activities, as well as by responsible individuals in organizations who have adopted a form of ERP mobility themselves, to controls risks they encounter due to mobility.

Keywords: Enterprise Resource Planning, Mobile technology, ERP mobility, Risk management, IT audit, Control framework

Acknowledgement

The duration of this thesis project was about 7 to 8 months, and during this period I have had help and support of a number of people. First and foremost, I have had tremendous help in numerous areas from three people in particular; my thesis supervisors. Floris Bex and Marco Spruit from Utrecht University as my internal supervisors, who helped me a lot with methodology aspects, scoping the project, and were always able to provide solid and to-the-point feedback. Ron Hakvoort from Deloitte as my external supervisor, with whom our recurring once-every-few-week meetings helped a lot with understanding the broader context of Risk Management, IT auditing, and information security, and who could always provide precise feedback and contacts at organizations (both internal and external) who have helped me throughout my thesis. This brings me to a next group of people I would like to thank for their time and knowledge; those who were willing to lend their knowledge to this research by allowing me to conduct an interview with them, and those who participated in the case study that was conducted to validate the research. These persons provided valuable insights into numerous aspects of this research, and have helped me construct the final deliverable of this thesis, and with that of my entire time as a student also.

On a more personal note I would like to thank my now ex-student colleagues from Utrecht University who have become good friends during the past few years, for making it a very pleasant time in the first place, but also for our insightful discussions in times when I needed an extra pair of eyes. Finally I would like to mention my girlfriend Lisette, who has supported me throughout my thesis period.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Research Trigger

Enterprise Resource Planning (ERP) systems are widely used and play a vital role in many organizations today. It comprises a set of integrated applications to manage the business and automate back office functions related to technology, services, and human resources (Gelogo & Kim, 2014). Adoption of ERP has reached a close-to-saturation rate in large enterprises (LEs) and more and more small and medium-size enterprises (SMEs) are adopting ERP systems, making them the most widely adopted system among large companies (Haddara & Zach, 2011). The concept of ERP systems however is changing due to the emergence and adoption of new upcoming technologies, such as mobile technologies. With adoption of mobile technology in businesses, many new (business) opportunities have arisen. (One) of the most significant features is the employee's ability to access corporate data via their mobile devices, allowing them to for instance retrieve production information on site, or send invoices on-the-go. Mobility is immensely popular, both in the consumer and enterprise environment. Moreover with mobility it seems to be the cast that technological advances hit the marketplace every few months rather than every few years (Mobile Security Collaboration Space Deloitte Global, 2014). This means that today's mobile ecosystem is a complex, rapidly developing environment consisting of different types of mobile devices, data communication channels, connectivity methods, and ecosystem actors. In essence, M-ERP (M-ERP) does not simply involve acquiring mobile devices for your employees and allowing them to send mails via these devices, or keep their calendars up-to-date on the go. M-ERP potentially changes the way organizations conduct their key business processes, and while business opportunities brought by mobile technologies are promising and extensive, it also brings new risks with it and potentially amplifies existing risks (Ernst & Young, 2013), threatening the security of (sensitive) data. Therefore, organizations adopting a form of ERP mobility, having insight in the risks involved with adopting such a system is of great importance.

While the topics of security, risk assessment, and risk management in traditional ERP systems and other Enterprise Information Systems (EIS) have already been established over the past few years, emerging IT architectures such as mobile computing platforms invalidate existing information assurance certifications (Breaux & Rao, 2013). A new look towards these security aspects and involved risks is thus required, yet studies examining M-ERP security are still lacking (Bradford, Earp, & Grabski, 2014). Enterprises adopting M-ERP solutions need to take into account the impact of mobility. New and amplified risks caused by mobility need to be mitigated and controlled to ensure secure integration of traditional ERP systems with mobile technology, into one working solution.

1.2 Problem Statement & Research Objective

While previous research on risk assessment in the more generic concept of enterprise mobility has been conducted (Janssen, 2013), there are few studies focusing on the impact of integrating mobility with traditional ERP environments. Moreover, there is no framework or model answering the question which different types of risks are involved with adopting a M-ERP solution, where these risks occur, and most importantly, how enterprise organizations can mitigate and control these risks. Because of the potentially large impact of mobile on enterprise organizations (Brockett, Golden, & Wolman, 2012), there is a need for a complete and comprehensive overview providing insight in the types of risks occurring due to ERP

mobility, one that is up-to-par with the current threat landscape surrounding the concept of M-ERP. Accordingly, the formal problem statement of this thesis project is:

IT auditors have no comprehensive overview of the risks involved with ERP mobility, and there is no existing model or framework that can be used as guidance to mitigate these risks and analyze the application and effectiveness of mitigating activities

The main objective of this thesis is to provide this comprehensive overview in a control framework. The framework defines different risk types that need to be controlled, and provides related control activities and procedures that can be implemented in organizations where ERP mobility is adopted, to counter these risks. The risk-control framework will allow enterprise organizations and IT-auditors to analyze the application and effectiveness of those controls that have been implemented in the organization, thereby assessing the state of their control activities, in terms of mitigating the risks related to ERP mobility in the organization. The main purpose of this framework is to provide IT auditors with insight in two aspects of ERP mobility, concretely:

1. **Risks** involved with implementing a M-ERP solution
2. **Control** activities that can be incorporated to mitigate these risks

The formal research objective of this thesis project is:

How can a risk-control framework be developed that addresses information security control objectives arising from risks to the confidentiality, integrity, and availability of information in M-ERP solutions?

1.3 Research Questions

From the elements defined above (chapter 1.2: Research Objective & Problem Statement), the following main research question (MRQ) can now be defined:

From an information security perspective, what is the impact of integrating mobile technology with existing ERP environments?

Four additional sub-research questions are formulated to answer the main research question, address the problem statement, and thus reach the research objective in this thesis project.

SRQ1: What different types of risk exist as a result from ERP mobility, and where do they occur?

Any control framework starts with identifying the risks that need to be mitigated, in order to determine the necessary controls that need to be implemented to mitigate these risks. Identifying important new risks as well as existing risks that are amplified or changed due to ERP mobility is key in this thesis, and provides the fundamental basis for the envisioned control framework.

SRQ2: How can each of the identified risks be mitigated and controlled?

The counterpart of risks are the controls that mitigate them. To determine the maturity of an organization in dealing with the risks that arise from ERP mobility, all possible controls activities, procedures, and mechanisms need to be identified that enterprise organizations can implement to mitigate the aforementioned risks.

SRQ3: To what extent can existing control frameworks related to IT risk and IT controls be used for ERP mobility?

Traditional control frameworks are evaluated to determine to what extent mobile information security in ERP solutions is already addressed. An evaluation of traditional frameworks is performed to determine which entities and components are of importance in the process of mitigating information security risks. Furthermore, this preliminary analysis contributes to a conceptual version of the envisioned control framework by adopting applicable elements from existing frameworks.

SRQ4: How do ERP mobility usage and strategies impact the type and amount of risks that need to be mitigated?

An analysis of how (strategies) and in what ways M-ERP solutions are being used (usage) is performed, to determine their impact on the risks that arise from ERP mobility. It is expected that different risks may need to be mitigated, depending on the kind of processes that are supported with mobility, the type of information being processed, and the way in which information is disclosed to the mobile device.

1.4 Scope

Enterprise risk management, enterprise mobility, and mobile security have all been, or still are popular topics in scientific research. However, research within each of these topics can have very different angles and different levels of scope, making it research areas on their own. It is therefore of great importance to determine and define a very clear scope as to what will and will not be part of this thesis project.

What will be part of this thesis project is:

- Areas and topics related to the evolution of ERP solutions, among others; adoption of ERP, internal controls, information security
- Risks affecting information security in ERP solutions as a result from ERP mobility
- Control activities, procedures, and mechanisms that can be implemented to mitigate these risks

- ERP mobility strategies: what information is disclosed via mobile devices
- ERP mobility usage: what business processes are supported with mobility

What will not be part of this thesis project is:

- Investigating specific topics related to mobile app development
- Elaborating on technical aspects related to information security (specific hacking & encryption methods, security protocols, and Identity Access Management (IAM))
- Reasoning on privacy and compliance issues (e.g. international regulations)
- Investigating different ways of implementing a M-ERP solution
- Investigating different enterprise mobility strategies
- Reasoning if and when M-ERP should be used
- Developing a mobile risk assessment method
- Reasoning on usability aspects in mobile enterprise applications
- Compliance and privacy aspects in ERP mobility

1.5 Definitions

As mentioned earlier, research related to Enterprise Risk Management, Enterprise Mobility, and Mobile Security, each can have very different angles and different levels of scope. Accordingly, terminology used in research related to these topics often have quite different interpretations. This section provides an overview and explanation of the key concepts relevant to this research, as they are interpreted and used throughout this thesis project.

#1 Enterprise Information System (EIS) – Within this thesis project, an EIS is considered to be any kind of information system that handles companywide information. When looking at the mobile infrastructure (defined in #5) of EIS, the EIS is typically the back-end system from which data is retrieved. Examples of EIS are ERP systems (defined in #2), Customers Relationship Management (CRM) systems, and legacy database systems.

#2 Enterprise Resource Planning (ERP) system – ERP is a type of EIS (defined in #1) that provides information on the core processes of an enterprise. An ERP system can be defined as a customizable, standard application software which includes integrated business solutions for the core processes and the main administrative functions of an enterprise (Klaus, Rosemann, & Gable, 2000).

#3 M-ERP – With the adoption of mobile technology, mobile solutions of ERP systems have emerged. Within this thesis project, M-ERP refers to the concept where employees can access ERP system data using mobile devices through the use of an app.

#4 Mobile device – Within this research project a mobile device is considered as a smartphone or tablet that cannot be managed like conventional computers and are not within the borders of the corporate building for a substantial amount of time (Janssen, 2013). This excludes for instance laptops.

#5 Mobile infrastructure – An information infrastructure is defined as all of the people, processes, procedures, tools, facilities, and technology, which supports the creation, use, transport, storage, and

destruction of information (Pironti, 2006). The mobile infrastructure refers to this infrastructure, specifically designed to include the usage of mobile devices (defined in #4) to access ERP systems (defined in #2).

#7 Risk – Within the scope of this study, a risk is defined as a negative event harming the enterprise, as a result of not properly setting controls (defined in #11) in place when implementing a M-ERP solution.

#11 Control – Activities, procedures, and mechanisms that mitigate a risk (defined in #7).

1.6 Scientific & Social Relevance

1.6.1 Scientific Relevance

ERP systems have been a subject of research for over 20 years, making it a very mature area of research. Much research has been done on ERP systems security, integration, implementation strategies, and change management (Al-Mashari, 2002). However, with the emergence and adoption of mobile technology, the ERP landscape is now in the process of fundamental change. However, with regard to M-ERP solutions, research is still lacking. One reason for this is simply because it is a type of solution not used that often yet by organizations, not on a large scale at least. Establishing a control framework resulting in the development of a dashboard specifically for M-ERP solutions contributes to the knowledge base of already existing control frameworks and models focusing on other domains or entities. It might also serve as a basis for further research where projects similar to this thesis can be performed, for instance aimed at different types of Enterprise Information Systems (e.g. CRM), or by extending this research by focusing on different types of risks (e.g. focused on regulatory compliance issues, due to the obligation of being compliant with national regulations in foreign countries).

1.6.2 Social Relevance

While most organizations use mobile devices for supportive processes (e.g. mail), only few are setting up or already have mobile device support for their primary processes, thus connecting mobile devices to their ERP system. Despite its potential, organizations are still hesitant to implement M-ERP solutions, mostly due to the fact that mobile security managers and experts consider data loss as a result of mobility in general a very considerable threat (Janssen, 2013). For M-ERP systems specifically, this is no different.

ERP systems such as SAP ERP provide a great deal of automation. When talking about M-ERP solutions this does not merely involve sending e-mails via mobile devices. M-ERP is more than that; it potentially changes the way organizations perform their primary business processes, allowing for better and faster decision making, and shortened operation cycles (Bar & Mohamed, 2011). With essentially all mobile devices facilitating a connection to the internet and thus access to the corporate information system (allowing manipulation and transfer of data), information security of M-ERP solutions becomes all the more important (Markelj & Bernik, 2012). Gaining insight in the different risk areas involved when implementing M-ERP solutions through a single model helps ERP solution providers in communicating such risks with co-workers and clients. More importantly, it provides (mobile) security professionals, IT auditors, and organizations who consider implementing a M-ERP solution, a means of understanding the

different information security aspects involved with M-ERP, as well applicable controls that can be incorporated to mitigate such risks.

1.7 Main Deliverables

The contribution of this research will be threefold:

- Insight in the risks involved with implementing M-ERP solutions;
- M-ERP Control framework (M-ERP CF) comprising the risks involved with implementing M-ERP solutions, the controls to mitigate these risks;
- M-ERP Dashboard (M-ERP Db) giving professionals and enterprise organizations a means to analyze the state of effectiveness of their controls related to risks arising from ERP mobility.

1.7.1 M-ERP Control Framework

The M-ERP control framework is a detailed framework linking risks to applicable controls, i.e. a template providing an overview of different areas where risks occur, which specific risks exist, and how each of these risks can be mitigated by one or more controls. The framework's main purpose is to provide a data structure organizing and categorizing internal controls that mitigate specific types of risks that arise from ERP mobility. Moreover, it could be used as a communication/advisory tool towards co-workers and clients because it specifies risks and controls on a very detailed level. The control framework is further elaborated on in chapter 6: M-ERP Risk-Control Framework.

1.7.2 M-ERP Dashboard

The M-ERP Risk-Control Dashboard is a dashboard that can be used to analyze the state of an organization's internal controls that have been implemented to mitigate ERP mobility risks. It presents a high level overview of the different areas that are relevant, and for each area it provides a set of controls that need to be implemented to mitigate the risks specifically in that area. Both the framework and dashboard are further elaborated on in chapter 6: M-ERP Control framework.

2 Research approach

This chapter describes the research approach followed throughout this thesis, and discusses the theoretical and scientifically justified methodologies that are used to conduct this research.

2.1 Research method

To achieve the research objective defined in chapter 1.2, and answer the research questions defined in chapter 1.3, a structured research approach is followed that follows the Information Systems Research Framework (ISRF) (Esearch, Hevner, March, Park, & Ram, 2004). The ISRF describes the design-science paradigm; "seeking to extend the boundaries of human and organizational capabilities by creating new and innovative artifacts". Since the main deliverable (M-ERP control framework) is a newly constructed artifact, the ISRF is applicable to this research. An overview of the thesis embedded the ISRF is depicted in Figure 1. According to the ISRF, Information Systems research goes through five phases:

(1) The research is triggered by a particular *business need* arising in the 'Environment' (left column in Figure 1). The business need for the present thesis was the lack of insight in the risks involved with M-ERP solutions. Professionals and enterprise organizations require insight in these risks so that they can properly mitigate them, and avoid the risks occurring and thus affecting their organization.

(2) A (scientific) knowledge base (right column in Figure 1) provides *foundations and methodologies* that are relevant to the business need, and can help solve it. For this thesis project the knowledge base consists of existing (IT) risk/control frameworks, capability maturity models, and theories that are relevant to the ERP mobility topic.

(3) Based on the two previous phases, the business need and (scientific) knowledge base, an *innovative artifact* is developed that addresses the business need (middle column in Figure 1). This thesis project's main deliverables are the MERP control framework and the MERP CCMM (as described in chapter 1.7), which are the artifacts that address the business need defined in stage 1.

(4) Finally, the artifacts that have been developed need to be justified and evaluated to ensure the *soundness and correctness* of the research. By means of a single case study at an organization in which a M-ERP system has been adopted (further elaborated on in chapter 2.5) as well as validation interviews, both internal and external validation is ensured.

(5) As a result, the artifacts developed in this research (control framework & dashboard) will *contribute to the knowledge* base as well as provide an *applicable solution* to the business need from which the research trigger originated.

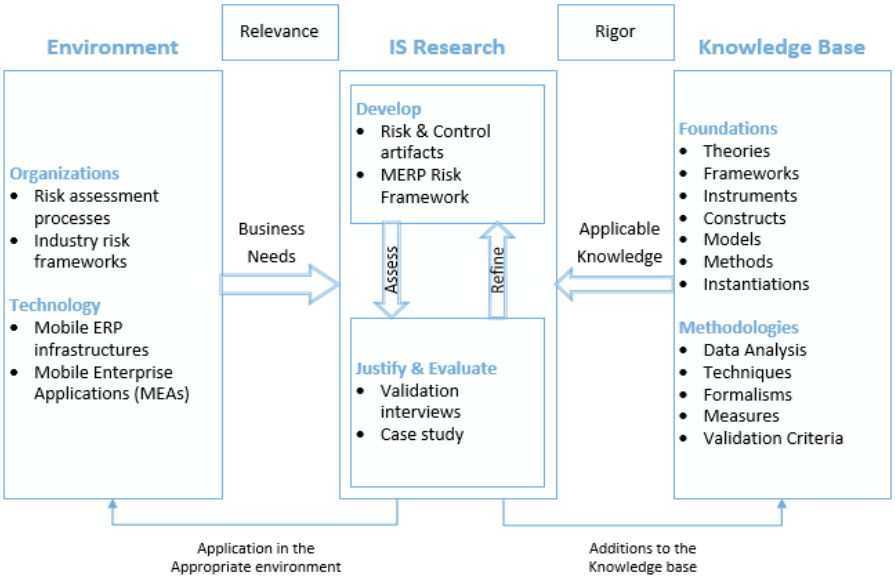


Figure 1 - Thesis Project within the Information Systems Research Framework (Hevner et al., 2004)

The research approach adopted for this thesis throughout this thesis project employs four different research methods. Each of the research methods contributes to the final development of the control framework, as well as the MERP CCMM. An overview of the research methods applied for executing this research is depicted in Table 1.

Research method	Domain/purpose
Literature study	• Existing IT risk/control frameworks • Existing Enterprise risk frameworks • Topics related to risks/information security of M-ERP (EIS)
Document study	• Mobile SAP Security • Enterprise mobility • Internal control • Industry control frameworks & templates
Interviews	• General security experts • (mobile) Security experts at ERP solution providers • (mobile) Security experts at organizations at which a M-ERP solution has been implemented
Validation interviews	• (mobile) Security experts at Deloitte
Case study	• Evaluation of proposed framework & maturity model

Table 1 - Overview of applied research methods

2.2 Research process

The research model depicted in Figure 2 is adopted from the research model method designed by Verschuren & Doorewaard (2007). It summarizes the main research objects for this research, elaborating on the middle pillar of the IS Research Framework shown in Figure 1. The numbers in Figure 2 (1 – 5) each represent one of the different research methods employed in this thesis project (as shown in Table 1). The letters in Figure 2 (A, B, C) each represent an iteration in the development process of the framework

and maturity model, that will be developed as a result of this thesis project. Dashed boxes represent the processes that result in deliverables, i.e. the applied research methods. Deliverables are represented by the solid lined boxes, i.e. the products of each iteration in the development of the artifacts.

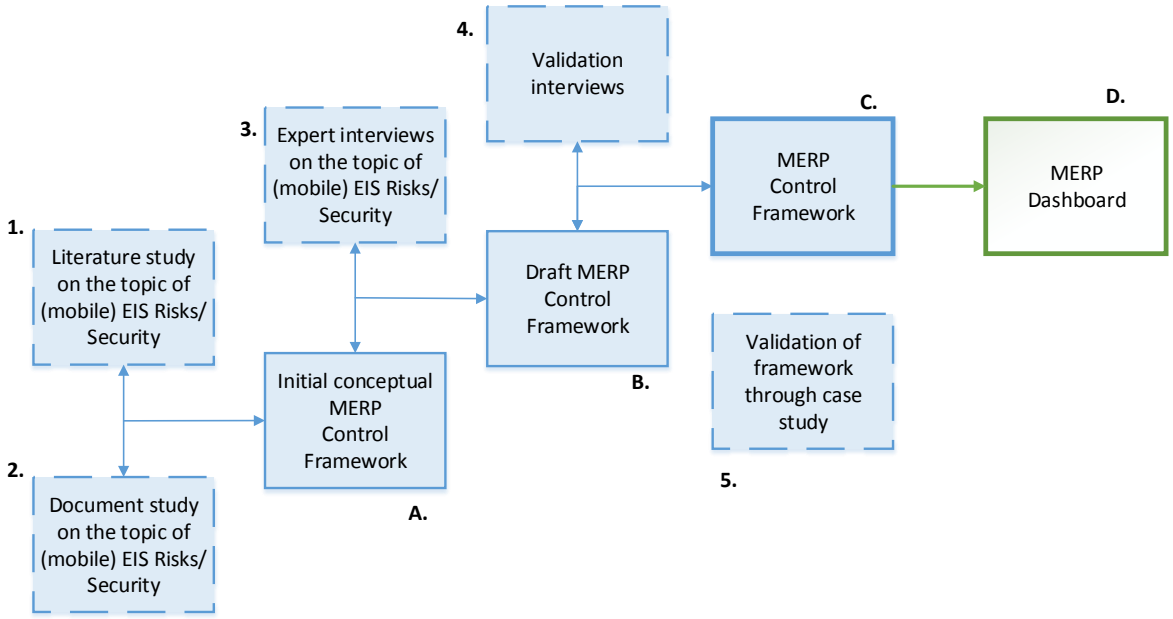


Figure 2 - Research model

2.2.1 Iteration 1: Systematic Literature Review

A thorough systematic literature study (SLR) has been performed on the topic of mobile EIS risks & security, with a primary focus on ERP systems. The literature study was performed using the methodology developed by Tranfield, Denyer, & Smart (2003), a method aimed at developing evidence-informed management knowledge (business) by means of systematic review, making it highly applicable to this thesis project. Their method of conducting a systematic literature review consists of three stages:

1. Planning the review

The first step in planning the systematic literature review is performing a scoping study, gaining a brief overview of the theoretical, practical and methodological history of debates surrounding the field and sub-fields. Based on this scoping study, a clear scope and focus (defined in chapter 1.4) is set, and clear questions that need to be addressed can be defined. Successively, a search strategy for identification of relevant studies to this research are defined, including the criteria for inclusion and exclusion of studies found in the review.

Criteria used throughout the SLR to include and exclude studies include were:

- Relevant to the scope described in chapter 1.4;
- Published after 2010;
- Derived from scientifically respected sources.

First of all, only studies relevant to the scope described in chapter 1.4 are eligible for inclusion. While this may seem obvious, lots of seemingly relevant studies have been performed related to mobile technology. The scope of some of those research areas however (e.g. the detailed workings of specific mobile encryption methodologies) is on a too specific level, making them largely unusable for detailed review in this thesis. Nonetheless, these studies have been analyzed on a high level, since controls can be derived from them. Secondly, only studies published after 2010 (i.e. in 2011, 2012, 2013, and 2014) are eligible for inclusion in the SLR. A time-span of only three years is chosen because of the novelty and innovative nature of this research area. This means that research on M-ERP risks is an immature topic of research, partly because it is an area still very vibrant and constantly changing. In turn this causes research to become outdated more quickly compared to other more mature areas of research. Lastly, only studies derived from scientifically respected sources are eligible for inclusion in the SLR. Again due to the novelty and innovative nature of this research, plus the fact that it is a very hot topic in the corporate environment as well, lots of business reports from sources such as Gartner and Forrester are found. These publications can be defined as so-called 'grey literature' (Petticrew, 2006). While these publications are thus not explicitly used in the SLR, they are however used to backup statements, either derived from the SLR or expert interviews.

2. Conducting the review

Built from preliminary reading of literature and the scoping study performed in the previous stage, keywords and search terms were identified that were found to be most appropriate to achieve optimal results. Reporting of the search strategy (keywords, search terms, search strings, results) should be done in sufficient detail to ensure that the search could be replicated. Therefore, keeping track of the SLR strategy was performed in an Excel-template, ensuring all activities during the execution stage of the SLR are documented.

The first step in conducting the review was including and excluding studies that were found when using the search strings deemed most appropriate. Based on reading the titles of all the papers found when using the search strings and following the criteria defined in the previous stage, 151 potential paper were found and included in a first set of potential papers for the SLR. This set of 151 potential papers were then all analyzed on relevance to the topic of study by reading their abstracts, and occasionally scanning through the paper. From this analysis a final set of 54 papers were identified that were deemed relevant to the topic of study, and thus included in the final subset of papers that are used in the SLR. For the remaining 97 papers that were excluded, reasons for exclusion were documented.

3. Reporting and dissemination

The final stage of the SLR is reporting the findings from the studies that have been included (further elaborated on in chapter 3). The findings essentially represent a descriptive analysis of the field of research, categorizing the 54 papers into five sub-topics that capture the research areas relevant to this thesis project, within the scope defined in chapter 1.4:

(1) Mobile enterprise applications
(2) Evolution of ERP and EIS systems
(3) Adoption of mobile technology
(4) IT auditing & internal controls

(5) Information security

Based on the findings from the SLR a first version of the control framework is established, that also serves as a basis for the interview protocols used in the expert interviews. As already mentioned, substantive results were also found that can be described as 'grey literature'. These publications have been added to the collection of other business reports and industry oriented research publications. Studying these publications and reports complements the results of the SLR as well as those from the expert interviews.

2.2.2 Iteration 2: Expert Interviews

The main input besides the SLR used for the development of the envisioned control framework and CMM, is obtained by conducting expert interviews. Because of the innovative nature and the fact that the research field has not been explored enough to set up a grounded survey based on theoretical foundations, a qualitative approach is chosen (Jacobsen & Hellstorm, 2002). Interviews will be conducted with three distinctive parties:

(1) (mobile) security experts at ERP solution providers
(2) (mobile) security experts at organizations that have implemented a M-ERP solution for their day-to-day business activities
(3) (mobile) security experts at a an organization that advises clients on how to mitigate risks arising from ERP mobility

For all three parties a different interview protocol is designed and can be found in Appendix D. The interview protocols serve as a guidance for the interview. The essential topics are included, yet also leaving enough room and time for spontaneous input from the interviewees.

The initial conceptual control framework is adjusted based on insights gained from these interviews. Expected is to gain insights from the expert interviews leading to substantial adjustments of the control framework content-wise, and possibly structurally as well. After having established a draft version of the control framework and developed a dashboard based on its contents, informal validation interviews will be conducted with security and experts and IT audit professionals at Deloitte to ensure the correctness and applicability of the framework.

2.2.3 Iteration 3: Case Study

The third and final iteration in the development process of the control framework and the maturity model derived from it will consist of a case study. The reason for conducting a case study is to evaluate the proposed framework and maturity model in practice. Moreover, it will serve as a final external validation that complements the internal validation interviews with security experts and IT auditors at Deloitte. The case study organization evaluated ought to be an organization that has implemented a M-ERP solution, and more importantly it should be a case that is representative for comparable situations (Cavaye, 1996).

SAP is by far the biggest global ERP solution provider with a market share of 25% in the Worldwide ERP Software Market in 2013 (Columbus, 2013), at the time nearly doubling the market share of its next competitor in this market (Oracle with a 13% market share). Due to SAP ERP's complexity and the fact that it is the ERP solution mostly used in enterprise organizations, finding a case organization who has

implemented a mobile SAP ERP solution is a good way of ensuring external validation. In the case study the MERP control framework and MERP dashboard will be tested in practice. This is done by applying the control framework at the case study organization as if an actual audit would be conducted. Findings obtained after applying the control framework serve as input for the MERP dashboard, which is then used to analyze the application and effectiveness of implemented controls in the case organization.

2.3 SLR search results

Conducting the SLR started with a set of keywords (as described in section 2.2.1), that were used as input for the further SLR process, and have been defined as followed:

- "Mobile Enterprise Resource Planning"
- "Mobile Enterprise Information System"
- "Enterprise risk"
- "IT risk"
- "Mobile security"
- "Risk framework"
- "Information security"
- "Data security"
- "Mobile infrastructure"

These keywords have been entered separately in Google Scholar to assess which topics would come up most as a result, and thus would be most relevant to the set of keywords. By analyzing the top 10 results, or in any case, those results appearing on the first page, a set of topics was defined. The set of topics led to the categorization depicted in Table 2. These topic categories were thus derived from entering each keyword separately into the search engine.

Seven categories were created, representing the array of topics in literature related to the keywords. Specific topics within the different categories were then combined to create a set of final search strings. These search strings were used as input to find the actual publications that were to be read for the thesis.

Category	Topics
Enterprise mobility	Mobile infrastructure
	Enterprise mobility
	Mobile enterprise platform
	Mobile enterprise
	Mobile environment
Data	Enterprise data
	Mobile data exposure
	Data storage
	Secure data processing
Application	Application security
	Mobile enterprise application
	Enterprise mobile computing
	Mobile application

Category	Topics
General ERP	Security and privacy
	Evolution of ERP
	ERP adoption
	M-ERP adoption
	Mobile information system
General security	Security protocol
	Authentication
	Trust management
	Access policy framework
	Mitigate enterprise risk
	Security risk assessment
Cyber risk	Cyber risk
	Cyber threats
	Cyber risk detection
	Security risk analysis
Mobile device	Mobile device user
	Mobile device security
	Mobile device security requirement

Table 2 - Clustering of initial SLR topics

Based on the used search strings a first set of 61.969 papers was found. These papers were either in- or excluded based on possible relevancy and usability as interpreted from the paper titles, and the ability to directly download the papers. This in turn resulted in a second set of 151 papers deemed relevant and applicable based on their title. This set of papers was then again analyzed for relevance and applicability, by reading the abstracts of all 151 papers, and occasionally screening through the paper if unsure. Reasons for exclusion are documented when papers are not excluded. This exclusion round led to a final list of 54 papers that are used in the SLR. These papers were then again categorized to depict the main important topics within this thesis project found in literature, depicted in Figure 4. An overview of the entire SLR process is depicted in Figure 3.

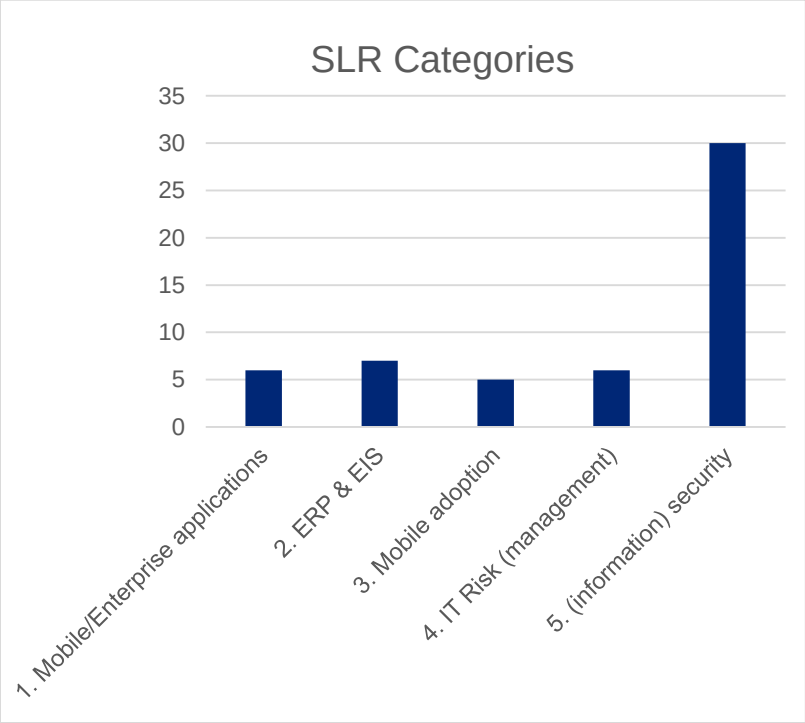


Figure 4 - SLR topic distribution

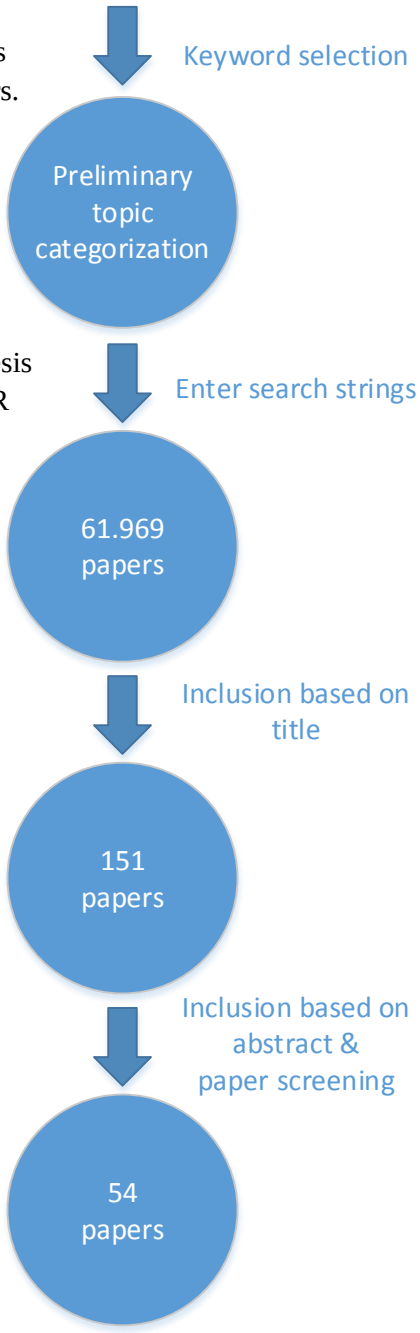


Figure 3 – SLR process

3 Theoretical background

This chapter elaborates on the theoretical concepts that are relevant to this thesis, describing the output of the SLR as described and discussed in sections 2.2.1 and 2.3 respectively. In addition, results of the document study are discussed, so that all the concepts relevant to this thesis are elaborated on in detail. These concepts capture the theoretical foundation needed to develop the risk-control framework for M-ERP risks, as well as the dashboard based on its contents.

3.1 Mobile Enterprise Resource Planning (M-ERP)

Nowadays, ERP solutions are widely used by large organizations around the world (Unhelkar, 2010), with adoption of ERP solutions reaching a close-to-saturation rate in large enterprises (LEs), and more and more small and medium-size enterprises (SMEs) adopting ERP solutions as well (Haddara & Zach, 2011; Xu, 2011). According to Xu (2011), not only large and medium sized companies but now also smaller companies are learning that a highly integrated ERP system is a requirement for global operations. But, what exactly is an ERP system? There are numerous definitions explaining the concept of an ERP system. Bar & Mohamed (2011) define the organizational process 'Enterprise Resource Planning' as "the integration process for all business functions and processes in an organization". This may include several different modules such as Human Resources, Inventory, Warehousing, and others. Consequently, the systems used to support the process of planning enterprise resources integrates information across an entire organization, both internal and external, to allow for a seamless flow of information (Engebrethson, 2012). More specifically, ERP systems can be considered as an integrated computer based system, used to manage internal and external resources including tangible assets, financial resources, materials and human resources. This means that processes supported by or performed through these systems, are typically of critical importance, because they carry, process, and store sensitive data of the enterprise (Muchenje, 2012).

With the emergence of mobility, ERP systems have to evolve. Employees no longer need to be on site or in the office from 9 am to 5 pm. As a consequence of technological advances, it has now become possible to integrate various technologies, including mobile devices, into enterprise infrastructures. Largely driven on the opportunity provided by the internet to now work from anywhere in the world, and the fact that most activities supported by ERP systems are dependent on timely and accurate access to enterprise information and processes, the ability to work when away from a desktop computer has become a huge draw for an ERP system (Engebrethson, 2012; Furtmüller, 2013; Maan, 2012). Moreover, because the entire business value chain of an enterprise is often also geographically fragmented, the value of traditional ERP systems is significantly reduced without the necessary mobility support (Maan, 2012). This makes mobile-enablement of existing enterprise systems such as ERP systems a necessity. Schadler & McCarthy (2012) predict that business spending on mobile projects will grow by 100% in 2015 compared to 2012, and that in 2016 approximately 350 million employees will use smartphones (of which about 200 million will bring their own into the enterprise).

Essentially, mobile devices are not simply another device for IT to support with a smaller sized website or a mobile device screen-sized SAP application. Rather, mobile appears to be the manifestation of a much broader shift to a new system of engagement (Schadler & McCarthy, 2012), potentially changing how business is performed in radical ways (Maan, 2012). This can be in the form of simple administrative

tasks such as an employee registering his or her work hours. However, imagine more radical ways such as signing off invoices, placing and confirming orders, or retrieving sensitive sales or production information on a mobile device. The mobile device looks to become a new gateway to all resources an organization has, of any kind. With that, different mobility trends can be found. Kumar (2012) identifies five trends associated with enterprise mobility:

- Mobility becoming an integral part of any enterprise application
- Business applications will be able to run on any device, at any time, and any place
- More engaging mobile applications utilizing features of smartphones like touchscreens, camera, video, voice and other features into business applications
- Mobile applications will evolve to encompass end-to-end business processes (e.g. procurement to payment, talent management and sales to delivery) and a broad range of business users
- Further increase in complexity of mobile devices and platforms due to consumerization of IT (the gap between business and privately used IT is closing)

ERP systems have thus become accessible to a broad range of business users through a broad range of mobile devices. This means that the overall concept of ERP mobility ends up being a complex whole of different business users, enterprise applications supporting business processes, and underlying technology (including the mobile devices). Factors such as technology convergence, market demand for the newest smartphones, access to specialized mobility applications, and trends observed in the consumer mobility space influence this need for mobility severely. The actual reasons however that cause these trends to happen, is mainly found in the specific benefits that mobility provides to those who adopt the technology.

Along with the aforementioned mobility trends, Kumar (2012) presents four key benefits to ERP mobility: enforcement of best practices, real-time communication, improved productivity, and paring costs through self-service capabilities. Bar & Mohamed (2011) define similar benefits on a higher level, which in practice leads to three main benefits:
(1) **Better decisions** (due to enforcement of best practices and real-time communication possibilities): with mobility, organizations can make better decisions, by for instance enforcing employees to follow best practices through mobile enterprise applications. Employees can for example be asked to do so when executing transactions on a remote location.
(2) **Faster decisions** (improved productivity): With real-time communication between employees, as well as real-time access to corporate data, decisions can be made at an earlier stage. Employees with remote access to corporate data can for instance retrieve production information on-site, and use this in their communication to the client. Employees are able to decide where to go from there, in direct consultation with the client.
(3) **Shortened process cycles**: Faster decision making leads to shortened process cycles, which means that less communication and waiting is required between the 'field' and the office.

While this list of benefits is by no means exhaustive, it does present an overview of the essential benefits mobility provides. Furthermore, while the benefits of ERP mobility in enterprises are extensive and clear, some serious challenges have arisen as well that need to be taken into account. One of those challenges lies in the fact that different types of data are stored on an employee's mobile device. On the one hand there is corporate data, and on the other there is privately owned personal data. Both types of data need to be managed, where from an enterprise perspective, managing corporate data is especially important. This

data may also be of sensitive nature, for instance a set of daily financial sales reports, which means that losing such data can have a huge impact on the enterprise. Aside from the fact that this data can be stored on the mobile device itself, through mobile devices employees also have access to the back-end enterprise system, emphasizing the principle of mobile devices becoming a gateway to enterprise resources.

Further elaborating on the issue of managing access to corporate data, there is the challenge of managing different types of devices attempting to gain access to this data as well (Furtmüller, 2013). This challenge is especially prevalent in so-called "Bring-Your- Own-Device" (BYOD) environments, which represents an enterprise mobility trend where organizations allow their employees to bring their personally owned mobile device into the corporate environment. Different mobile devices will then connect to the corporate network, and moreover they will do so via different access points, all of which need to be managed and secured.

To summarize, challenges include: (1) access to corporate data, (2) locally stored various types of (sensitive) data, (3) diversity of access points, and (4) diversity of devices. Again, this list is by no means exhaustive, many more challenges can be found. One of those additional challenges lies in the fact that in the world of computers and communication, the more widely a technology is used, the more likely it is to become target of hackers (Leavitt, 2011). This introduces the risk of malware (malicious software); software designed to invade, spy on, or damage computer or other programmable devices (Umberger & Gheorghe, 2011). This can especially become an issue that needs to be addressed when considered in combination with the four aforementioned challenges, like managing different data types or access to corporate data.

All in all, the popularity and potential impact of mobile devices in the enterprise environment is enormous. It is clear that mobility has happened in the consumer environment, and it is happening in the enterprise environment as well. Traditional enterprise systems are being mobilized, and it has become a necessity for organizations to take into account the challenges that go along with that.

3.1.2 M-ERP infrastructure

This section elaborates on the different components that comprise a typical M-ERP environment. Three tiers are essentially distinguished (SAP, 2013):

1. EIS tier: enterprise information system and data sources
2. Server tier: middleware, development platform, mobile device management, mobile application management
3. Client tier : mobile device, mobile enterprise applications

Figure 5 shows an overview of the different components in the three tiers. Furthermore, a component called 'DMZ' is added, which is an abbreviation for de-militarized zone. In information security, DMZ is considered a sub-network that basically exposes the services provided in the server tier to a larger (untrusted) network; the internet (Bishop, 2000). The DMZ layer represents an additional layer of security for the organization, through which all data to and from the corporate network must pass through. This

means that potential external attackers must go through the DMZ layer, in order to access the content inside the corporate network.

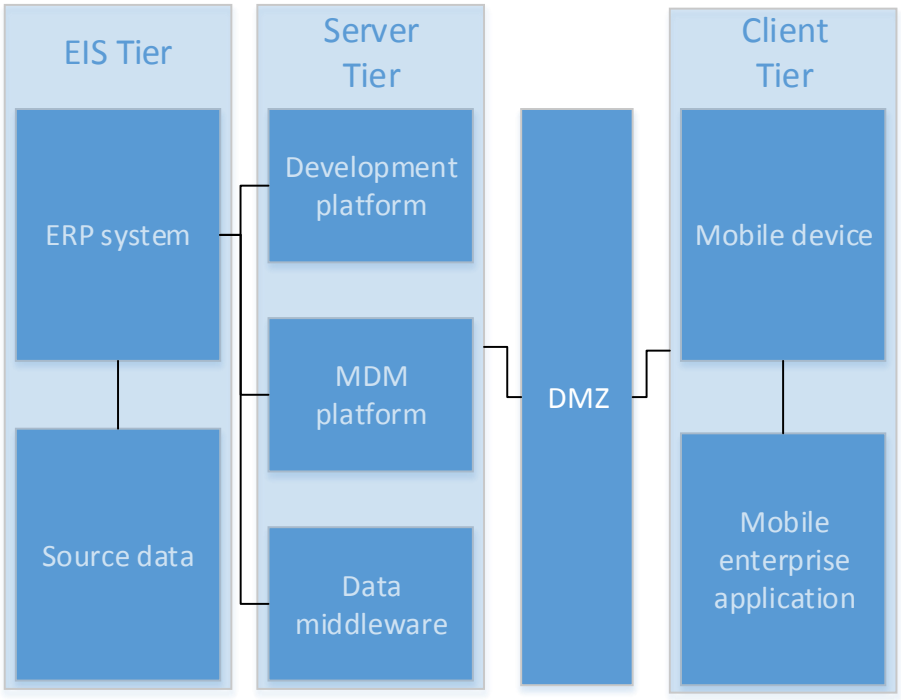


Figure 5 - ERP environment components (SAP, 2013)

One of the essential differences between traditional ERP infrastructures and those that include mobile devices, is the way in which communication can take place. Communication with mobile devices is different from traditional ERP solutions in four ways (Brockett et al., 2012): (1) the types of devices used, (2) the development languages, (3) communication protocols, and (4) the technologies used. While traditionally firewalls could set clear boundaries between the corporate network and the actors accessing the network, in current (mobile) IT infrastructures more communication paths need to be secured. Figure 6 highlights this difference in communication, emphasizing the fact that the corporate network infrastructure has changed; more diverse devices access the corporate network via more diverse communication channels. One of the consequences for organizations that support these different types of devices to access their system, is that different mobile operating systems need to be supported also, operating systems that for instance might use different mobile device encryption properties. On top of that, a majority of devices being used are often not updated to their latest available OS version (Lehrfeld, 2012). This means that even if an OS has proper security measures in their system, they can often not be relied upon in practice, simply because many users do not have them installed. In essence this depicts the tip of the iceberg when it comes to managing mobile devices in an ERP infrastructure supporting mobile device. Not only the devices themselves should be managed, but surrounding processes such as mobile OS version control need to be implemented, maintained and supervised also.

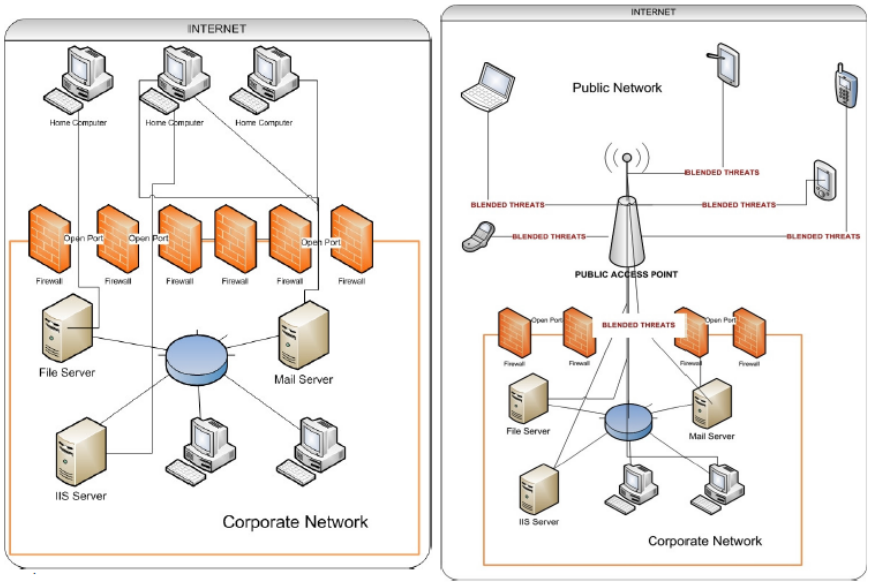


Figure 6 - Changes in communication with corporate network (Markelj & Bernik, 2010)

EIS Tier

The EIS Tier represents the area where the back-end Enterprise Information System is situated. The system is linked to source data in a database that is also used in the mobile applications used by employees. With support of mobile devices, in essence not all that much changes in this tier. Same roles, authorizations and security features may apply, such as role-based access control, that need not to be different when it comes to users accessing the system via different devices and access points (at least not from a back-end perspective).

Server Tier

The server tier consists of three main components: Data middleware, Development platform, and Mobile Device Management.

Data middleware

The data middleware component should connect different platforms and devices to the back-end ERP software in the EIS tier. The data middleware component acts as a mediator, enabling applications to consume content and business logic from the back-end ERP system. Besides merely acting as a mediator, it also determines which pieces of data are available to mobile users, and distributes the data according to a set of business rules.

Development platform

Gelogo & Kim (2014) state that the use of a development platform allows the organization to use existing web development skills to create mobile business solutions. By integrating messaging functionalities, mobile device sensors, and notifications, organizations can further develop their own mobile apps as an extension to their ERP system, with functionalities specifically designed by and for the organization.

Mobile Device Management

The Mobile Device Management (MDM) platform is an important component in any ERP environment, and deals with configuring mobile devices and making sure that relevant (IT) policies stay intact. Through

the MDM platform several aspects regarding mobile devices in an enterprise are continuously monitored and controlled. A Citrix report from 2013 (Citrix, 2013) states that an MDM platform should enforce tight control in seven ways:

- Configuring device settings and policies: such as device and application restrictions
- Provisioning devices: via self-service enrollment and centralized distribution of configurations, policy, and application packages/updates
- Securing assets: devices, applications, the network and data need to be secured with authentication and access policies, application and cloud service blacklisting and whitelisting, enforcement of secure application tunneling, and deployment of content- and context-aware mobile data loss prevention policies
- Separating data: data from corporate apps, from personal apps, and data on the user's mobile device through need to be separated by using container technology
- Monitoring: devices, infrastructure, service levels and telecom expenses
- Supporting users: with remote user device control and troubleshooting, along with the ability to remotely locate, lock, and wipe devices in the event of loss or theft
- Decommissioning services: by identifying devices that are inactive and (selectively) wiping them upon employee departure.

Essentially, MDM enables an organization to manage active corporate issued or personally owned mobile devices remotely. It furthermore allows organizations to check if devices are subject to jail breaking, and also (de-)install apps on devices remotely. The latter is considered an extension of MDM: Mobile Application Management (MAM). MAM manages aspects specifically related to the applications that run on a mobile device. This for instance includes automatic deployment of applications to mobile devices without user involvement. Another possible extension of the MDM platform is Mobile Information Management (MIM). It is a system component that manages the availability of information to different groups of employees. MIM components are also referred to as Mobile Asset Management components, in the sense that different information types processed through a system are considered information assets. A categorization of information assets from the ISO/IEC 27000 standard (ISO/IEC, 2007) can is added in Appendix A. Depending on how a system is designed however, the Mobile Asset Management component has significant overlap in functionality with the Data Middleware component.

Client Tier

Mobile device

Many different types of mobile devices nowadays exist, each with their own characteristics. Mobile devices as considered within this thesis include hybrid laptops, tablets, phablets, smartphones, but also other mobile devices specifically designed for one particular purpose (such as devices used in warehouse management to register stock information, so-called ruggedized computers). This excludes however larger laptop or desktop computers.

Mobile Enterprise Applications

Now that we have discussed the general concept of M-ERP systems and the different components in the mobile platform, let us zoom into mobile enterprise applications in more detail. Giessmann, Stanoevska-Slabeva, & de Visser (2012) define mobile enterprise application as: "applications that are designed for and are operated on mobile devices and which facilitate business users within core and/core support process of their enterprises". This is in fact almost similar to the definition of a traditional enterprise

application: “the type of IT application that companies adopt to restructure interactions among groups of employees or with business partners” (McAfee, 2006). The sole difference between traditional enterprise applications and MEAs, seems to be that MEAs are designed for and operate on mobile devices. According to Giessmann et al. (2012), the evolution of mobile devices and applications in the consumer market is the main factor influencing the market for MEAs, which is not very surprisingly, since employees are also private end-consumers.

MEAs have a disruptive effect on existing enterprise software solutions, and one of the biggest challenges from a technical perspective, is the adjustment of existing enterprise applications for mobile extension through the use of mobile enterprise applications (Giessmann et al., 2012). MEAs are ultimately used to ensure the benefits identified earlier in section 3.1 (better and faster decisions, and shortened process cycles). More specifically, MEAs tend to be used for 5 main purposes (Hasan, Gómez, & Kurzhöfer, 2013):

1. Mobile broadcast (large-scale information broadcast to employees): e.g. distributing advertisement and promotions
2. Mobile information (provides information requested by the mobile user): e.g. requesting time tables or internal job vacancies
3. Mobile transaction (eases and executes transactions): e.g. e-transactions or CRM transactions
4. Mobile operation (covers internal operational aspects of the business): e.g. inventory or supply chain management activities
5. Collaboration among employees and various functional units: e.g. employees from different functional units sharing and creating knowledge together

These functionalities essentially empower an organization’s employees. Applications may for instance also be accessible even when not connected to the back-end enterprise system (Gelogo & Kim, 2014), enabling employees to retrieve up-to-date information whenever and wherever they need. This then results in supplier and inventory data always being accessible, streamlining the supply chain, and improving customer engagement by providing real-time sales and service information.

Giessmann et al. (2012) classifies MEAs according to five characteristics; target group, price, functional area, connectivity, and core business of application provider. When considering the risks arising from ERP mobility, especially the connectivity characteristic is important, since it represents the different ways in which information can be disclosed from the back-end enterprise system to the mobile device. Generally speaking there are three different connectivity types defined in terms of the client type the application uses: standalone applications, smart or full clients, and thin clients. These connectivity types are indicators for the extent to which the application has control over the information that is being accessed. Standalone applications for instance do not need any connection in order to provide their full range of functionality, meaning that information is accessed or modified by the user, independent of the fact whether or not the device is connected to the corporate network. Without a connection to the corporate network however, users will not be able to work with the latest data. Smart or full clients have a wide range of functionality within the application itself as well, so that the application can be operated both in connected and disconnected mode, but it requires a connection to synchronize data and be used to its fullest. Thin clients finally do not function without a data connection, and can thus only operate when connected to the back-end enterprise system. Based on different connectivity types, different data is

stored on and accessed through the mobile device. This further complicates the challenge of storing different types of data and accessing corporate data through the device, since each connectivity type requires a different approach in terms of managing the information being processed. Moreover it is not self-evident that mobile applications are used as pointed out by an interviewee (SUP02). Depending on the type of process and information supported with mobility, an organization may choose to use mobile responsive websites instead of native applications, or a mixture of the two.

Another goal for organizations is to maintain the accuracy and reliability of data within the ERP system (processed and modified through MEAs), so that the transparency of the company's situation at all times can be ensured. This transparency is needed to help (re)build investor confidence, and to ensure low cost of capital (Chuprunov, 2013). However, mobile device's physical limitations often force mobile application developers to make security and performance trade-offs. Limited power, processing cycles, memory, and bandwidth can force developers to give up security features like encryption in order to improve online performance. Use of lower level languages for phone communication development, as well as their often lacking built in non-functional security requirements, cause a continuation of software vulnerabilities (Freeman, 2011).

So while it appears that both in the scientific and business environment it is widely agreed upon that the use of MEAs offers extensive benefits and functionality for employees, security of mobile applications has become all the more important. The distinction between corporate and personal use of mobile device is becoming blurred, and apps both store and process a lot of sensitive personal as well as corporate information. With new technologies being used in MEAs (e.g. Near-Field-Communication (NFC) and QR-codes) new attack vectors, challenges and risks emerge as well (Jain & Shanbhag, 2012). All of these challenges have the potential to disrupt the use of a M-ERP system and affect the information processed within, thus denying an organization the benefits it provides. In organizations where the process of implementing a proper information security system to manage these challenges is not taken seriously, the value of mobility will be lost.

3.2 Information security

The ISO/IEC 17799 standard defines information security as: "the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities". The focus in this thesis is on identifying important risks involved with M-ERP solutions, and thus finding threats that somehow affect information of an enterprise, specifically due to the integration with mobility. When it comes to protection of information from this wide range of threats, in software systems it is often based on the three information security goals within the well-known CIA-triad: Confidentiality, Integrity, and Availability (CIA) (Figure 7). While the exact origins of the 'CIA triad' appear to be unknown, underlying concepts were already operative in military concepts millennia ago, well before the concept of 'information security' as we now know it came to existence. The ISO/IEC 27002:2005 standard defines information security as the "preservation of confidentiality, integrity, and availability of information". Avizienis, Laprie, Randell, & Landwehr (2004) define the CIA principles as follows:

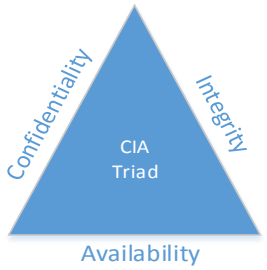


Figure 7 - Information security goals in the CIA-triad

Confidentiality: the absence of unauthorized disclosure of information
Integrity: the absence of improper system or data alterations
Availability: the readiness of systems to deliver correct services

When reasoning about information security, it is good to focus on enterprise information security goals rather than just the technologies (Julie & Ryan, 2011). To achieve these goals, having a proper information security system in place is imperative, and it is everyone's job within an organization to help achieve these goals, not just that of the IT or security department. This implies that all employees need to contribute in order for an organization to reach its information security goals. In this thesis information security is therefore also based on the CIA dimensions. Risks are hence also considered in terms of their potential and impact to affect one of the aforementioned security goals; either the confidentiality, integrity, or availability of information in a M-ERP environment (or a combination of those). A risk affecting the confidentiality of information for instance could mean that information is disclosed to a person who does not own the required authorization(s). Table 3 presents a more detailed overview of the three information security goals within the CIA-triad.

CIA principle	Definition	Example
Confidentiality	The absence of unauthorized disclosure of information	A hacker hacks into the enterprise information system. The hacker confiscates a dataset including sensitive corporate data. The confidentiality of the corporate data is no longer ensured.
Integrity	The absence of improper system or data alterations	A random employee has access rights in the enterprise system to the extent that he can get into data belonging to a different department. He does not have the required knowledge to work with the particular information, yet he can, and does do so. Because of his lack of know-how to work with the information, the information is changed on wrong assumptions. The integrity of the information can no longer be ensured.
Availability	The readiness of the system to deliver correct services	A group of hackers decide to target a server with an unusual large amount of server requests. The increase in the amount of server requests causes the servers to overload, meaning that all bandwidth is consumed by the server requests initiated by the hackers. There is no bandwidth left to process requests from legitimate users. Information is no longer available.

Table 3 - Information security goals overview (CIA)

To highlight the importance of information security, and put things into perspective: a report done by Symantec has valued global losses due to cybercrime in 2011 at 399 billion USD with 441 million people worldwide being affected by it (Norton, 2011). That means that in 2011, cybercrime globally cost the world a much greater amount than the global illicit trade in marijuana, cocaine and heroin combined, which is valued annually at 288 billion USD (Norton, 2011). Furthermore, even though statistics on cybercrime and threats to IT are already quite astonishing on their own, it is even unlikely that they cover the entire threat landscape (Choo, 2011), because statistics on cybercrime probably do not represent the full extent of cybercrime and the current threat landscape. Victims may for instance not be aware that their organization had experienced an incident, and they would then thus not indicate they had

experienced an incident when asked (even though they did). Additionally, organizations might have a fear for negative publicity, and might believe that reporting they had experienced an incident would result in a competitive disadvantage, causing them to not truthfully admit to incidents that had occurred (Richards, 2009).

3.2.1 Risks

There are numerous risks that can affect the confidentiality, integrity, and availability of information in information systems, and several definitions exist when it comes to risks affecting an enterprise. Freeman (2011) defines a risk as: "any uncertainty about a potential future event that threatens the enterprise's ability to accomplish its mission, endangers its core assets, and limits the organization's ability to provide critical services". He defines operational risk as: "concerns emanating from corporate IT and business processes", and states that these risks are increasingly centered on automated processes and information systems. The ISO/IEC 27005:2008 standard defines a risk as "a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event". From these definitions, a risk can thus be considered as the product of two factors: (1) the consequences (or impact) of an unwanted event, and (2) the likelihood that such an unwanted event will occur. In this formula impact is defined as "a measure of the effect of an event" (ISO/IEC, 2007).

This breaks a risk down into two questions; how likely is it that a particular risk will occur (likelihood), and what will this mean for the organization if this is not managed (impact). From another perspective, a risk can be defined in terms of two sub-elements that together actually compose a risk, the actual elements that cause a risk from occurring; threats and vulnerabilities. Many different definitions exists of both threats and vulnerabilities, summarized in Table 4.

Source	Threat	Vulnerability
ISO/IEC 27000	A potential source of an incident attack that may result in adverse changes to an asset or group of assets of an organization.	A weakness of an asset that can be exploited by a threat.
CIS 200701	A potential cause of an unwanted event that may result in harm to an organization.	A characteristic (including a weakness) of an information asset or group of information assets that can be exploited by a threat.
NIST	Actions or events (intentional or unintentional) which, if realized, will result in waste, fraud, abuse, or disruption of operations. Threats are always present, and the rate of threat occurrence cannot be controlled. Therefore, IT security safeguards, must be designed to prevent or minimize any impact of the affected IT system.	Weaknesses in an IT system's security environment. Threats may exploit or act through a vulnerability to adversely affect the IT system. Safeguards are used to mitigate or eliminate vulnerabilities.
ENISA	Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.	The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

Table 4 - Threat & Vulnerability definitions

Based on these definitions a threat is considered as any entity (in- or outside the organization), that can exploit a weakness of a system to cause (un-)intentional damage. Threats can thus exploit weaknesses in the system to cause some sort of damage, and manifest into a risk (resultant impact). A vulnerability represents the weakness that can be exploited of an asset or control, by one or more threats. Figure 8 depicts the relationship between threats, vulnerabilities, and risks in the context of information security. To illustrate this, let us look at the following example: a virus attacks a system with outdated anti-virus software. Because the anti-virus software in the system is not up-to-date, it does not have the necessary capabilities to fend off the virus. Sensitive information may now be stolen or modified by the virus, affecting the confidentiality and integrity of the information that is processed. In this example, the fact that the antivirus software is not up to date is considered a weakness in the system, and thus a vulnerability. The virus itself is considered as a threat that is able to exploit this vulnerability, i.e. exploiting the fact that the anti-virus software is not up-to-date and thus not capable of fending of the virus. Loss of data, system crashing, or compromised data are all potential risks that could occur as a consequence. This can however be avoided, or at least the likelihood of it happening can be minimized, if the anti-virus software is being kept up-to-date.

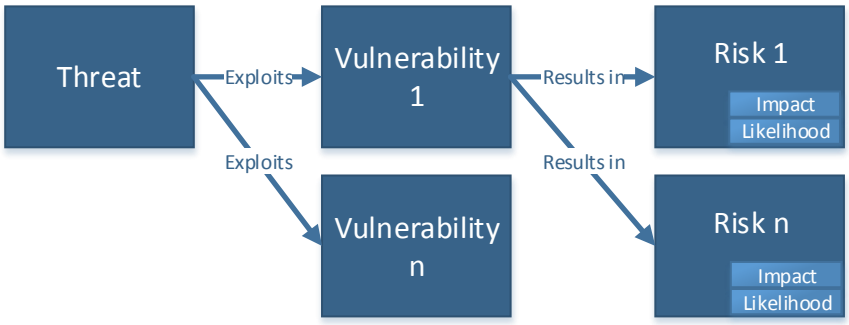


Figure 8 - Threat-Vulnerability-Risk relationship

An investigation by Verizon in 2012 (Verizon, 2012) dug into who the actors were behind a large number of data breaches in the US in 2012. Additionally, they investigated how these data breaches occurred, and what the commonalities between these breaches were. Table 5 shows an overview of their findings. Interesting to note is that the actors initiating a data breach are often from external sources, but a substantial amount of breaches were likely caused by business partners or vendors (32%), and a lesser but still significant amount, was caused by insiders of organizations who participated in the investigation (20%). Also, four distinct types of threats were found: (1) hacking & intrusions, (2) malware, (3) privilege misuse, and (4) physical threats. Stunningly, 87% of the breaches that were caused by one of the initiators through one of the four threat types, were considered to be avoidable through relatively simple counter measures.

In the Verizon investigation on data braches threats were considered as intentional threats, i.e. deliberate attacks aimed at retrieving or modifying data. More comprehensively, Choo (2011) distinguishes three different types attacks:

- Syntactic: exploiting technical vulnerabilities in software and hardware
- Semantic: exploiting social vulnerabilities
- Blended: using technical tools to facilitate social engineering

Who	How	Commonalities
20% caused by insiders	67% were attributed to a significant error	69% involved data the victim did not know was on the system/device
74% resulted from external sources	64% resulted from hacking and intrusions (mainly SQL and default credentials)	81% of victims were not Payment Card Industry Compliant (credit card standard for merchants/processors
32% implicated business partners or vendors	38% incorporated malware	83% of attacks were not highly difficult
39% involved multiple parties	22% involved privilege misuse	87% were considered avoidable through simple controls
	9% were due to physical threats	99.9% of records were compromised from servers and applications

Table 5 - Numbers on data breaches (Verizon 2012 Data Breach Investigation Report, 2012)

Threats can however also be unintentional, for instance due to errors and mistakes from personnel, that could lead to a loss of corporate data. It even appears to be the case that while intentional attacks are decreasing, the extent and impact of unintentional misuse increases heavily, at least in terms of the damage they cause (Verizon, 2012). These unintentional threats mostly occur because employees do something they should not have done. Threats can however also originate from other sources, most prominently technical, environmental/physical, and natural threats. With regard to human threats however, the originating source of events potentially posing a risk can further be divided as internal ones (initiated from within the organization, i.e. employees) or external ones (initiated from external sources, e.g. a hacker). The reason why the risk of events happening from internal sources (employees) is relatively high, is underlined by Brockett et al. (2012) with this statement: "While an employee can be a company's greatest asset, employees are constantly exposed to vast amounts of confidential information and are, by necessity, trusted with proprietary company information, inventory and property". In other words, employees are exposed to company data, because they need to have access to this data to do their job.

Besides that fact that employees simply require access to data for their work, they typically also have good knowledge of the vulnerabilities in their own information security system, making it relatively easier to exploit such flaws. A famous example of this is the case of the French bank Societe General, in which an insider had committed fraud for over €4.9 billion. A trader of the bank who had also worked in other departments (among others the IT department) had in-depth knowledge of systems and procedures, enabling him to avoid being detected by them. On top of that, it appeared that staff did not systematically conduct in-depth investigations when red-flags were raised, enabling the fraudulent employee to go about his business unnoticed.

In essence these internal sources may pose all kinds of risks. As in the example of Societe General, employees are tempted by individual gain (e.g. monetary), but employees may also simply believe to have a right to a particular information asset, because he or she spent time developing it (Brockett et al., 2012). This means that while employees can indeed be a company's greatest asset, an organization should implement an information security strategy based on the assumption they cannot always be trusted. Not just due to the fact that they may intentionally affect security of information, but also unintentionally by

for instance being victim to social engineering attacks, where employees may even not be aware of being attacked at all.
Kouns & Minoli (2011) identify a number of other distinctive risks to general information security, most prominently leakage of information. Information leakage can occur in many different ways, for instance due to unauthorized/malicious software, uncontrolled use of portable devices and transportable computer media (e.g. USB memory sticks, Blue-tooth-enabled devices), with some potential for deliberate attacks propagated on such devices/media (Trojan-infected USB sticks, CD-ROMs, etc.). By other means it could also be something as seemingly simple as theft and loss of mobile devices storing data. Many of these ways of leaking information could lead to identify theft of employees, especially in case it considers personal information. Other consequences could be about matters such as criminal prosecution, regulatory fines, and loss of public confidence in trusted organizations.

Two factors seem to heavily increase the chance of information actually leaking: social engineering and lacking information security studies (Kouns & Minoli, 2011). Social engineering, or targeted phishing and malware attacks, could be aimed to obtain unauthorized access to personal data, which then can be exploited by attackers for identity theft. On the other hand, lacking information security studies contribute to this matter also: a lack of risk assessments/projects may for instance cause failed, wasteful, excessive, or otherwise inadequate monitoring and auditing.

Risks arising from mobility

With regard to mobile devices, the three information security goals can be tailored towards mobility. The National Institute for Standards and Technology (National Institute of Standards and Technology, 2014) states that confidentiality with regard to mobile devices is about ensuring that data in transit and data at rest cannot be read by unauthorized parties, integrity about detecting any (un-)intentional changes to this data, and availability about ensuring that users can access resources using their mobile devices whenever they need to.

Because of this link between the device and the enterprise system, data is potentially being stored both in the system as well as on the device itself. Since mobile devices also facilitate access to corporate information systems, and also allow for manipulation and transfer of this data, keeping data that is stored on a mobile device secure is a critical requirement. It might even be the case that the data accessed by the device is more valuable than the device itself (Jain & Shanbhag, 2012; Markelj & Bernik, 2012). The need to secure a mobile device is also emphasized by the fact that any information system can be considered as safe as its weakest link (Markelj & Bernik, 2012), making it important to focus on the least controllable elements in your information system. This gives mobile devices a high priority in the entire system's infrastructure.

Furthermore, criminals appear to be turning their attention to mobile devices, because they are now the next generation of computing devices and have become the dominant computing platform (Sadeghi, 2013). This means that attackers target mobile devices, because end-users are using them more and more, resulting in an increase in threats now targeting mobile devices (Jain & Shanbhag, 2012; Kapko, 2012). Based on the differences between traditional and M-ERP environments, numerous amplified or altered threats have also emerged, that too pose a risk to the information security goals of any system (Ernst & Young, 2013).

Substantial research backs up the importance of information security in M-ERP environments. Malware for Android for instance increased by 350% in 2012 (Trend Micro, 2012) and now exceeds PCs in terms of malware attacks in the USA (Mansfield-Devine, 2013). Leavitt (2011) shows that the number of threats to mobile devices already increased drastically in 2011 (Figure 9).

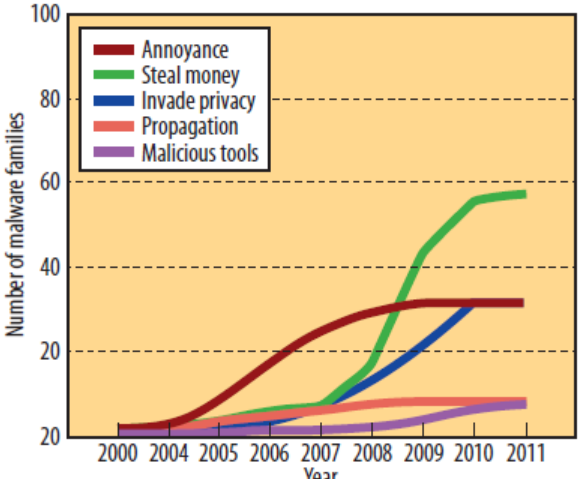


Figure 9 - Number of mobile device malware (Leavitt, 2011)

In any case from an enterprise point of view, the essential idea is that enterprise resources (corporate data) need to be protected from various threats that try to access, modify, or steal those resources. In other words, enterprises want to protect their resources from events that impact the confidentiality, integrity, and availability of those resources. For ERP mobility in specific, it can be stated that there are various enterprise resources access through mobile devices that may be subject to threats, and thus protection needs to be placed between them (Markelj & Bernik, 2012).

While this perception of threats to mobile enterprise information systems perfectly depicts the way in which threats can affect enterprise resources, it is too simplistic to capture the complexity and variety of risks affecting resources of an organization. The special NIST 800-124 publication defines 7 assumptions organizations should live by when considering the risks to information security due to use of mobile devices in an enterprise (Scarfone, Karen; Souppaya, 2013):

1. Mobile devices will be acquired by malicious parties who will attempt to recover sensitive data either directly from the devices themselves or indirectly by using the devices to access the organization's remote resources. Even if always in possession of the owner, attackers could look over a shoulder to see sensitive data – such as a password being entered.
2. All mobile devices are untrusted unless the organization has properly secured them and monitors their activity continuously while in use with enterprise applications or data.
3. The networks between the mobile device and the organization cannot be trusted.
4. Unknown third-party mobile device applications downloadable by users should not be trusted.
5. Mobile devices may interact with other systems in terms of data exchange and storage that are often external.
6. Mobile devices may use untrusted content other types of devices generally do not encounter, such as QR codes.
7. Mobile devices with location services enabled are at increased risk of targeted attacks.

These assumptions all somehow relate to the mobile device. Either the device itself (1, 2, 7), applications running on the device (4, 6), data on the network to and from the device (3), and the device's environment (5). This already implies that threats to information security in a mobile environment not only have to do with the mobile devices themselves, but also other aspects play part, such as data, network, and the

environment of the device. The devices themselves are merely the end points in the entire ERP mobility infrastructure, as discussed in section 3.1.2.

Jain & Shanbhag (2012) divide threats in a mobile environment in 7 categories (Figure 10). While not all threats are unique for a mobile environment, some of these threats do gain more prominence in a mobile environment compared to traditional ERP environments, especially threats such as device loss, data interception, and malware. In information security in mobile environments, the user of the mobile device appears to be the number one weak link. In combination with the absence of standards set by the organization for the use of hardware and software, this poses serious risks (Markelj & Bernik, 2012). This mainly involves risks regarding the software and applications for mobile devices, the networks they use, but also usage of unprotected certificates, and malicious insider attacks (Lehrfeld, 2012; Markelj & Bernik, 2012). Other prevalent security concerns with mobile devices are found to be Jailbreaking & Rooting of devices, and mobile device platforms and markets such as Android and iOS (Harris & Patten, 2014; Leavitt, 2011).

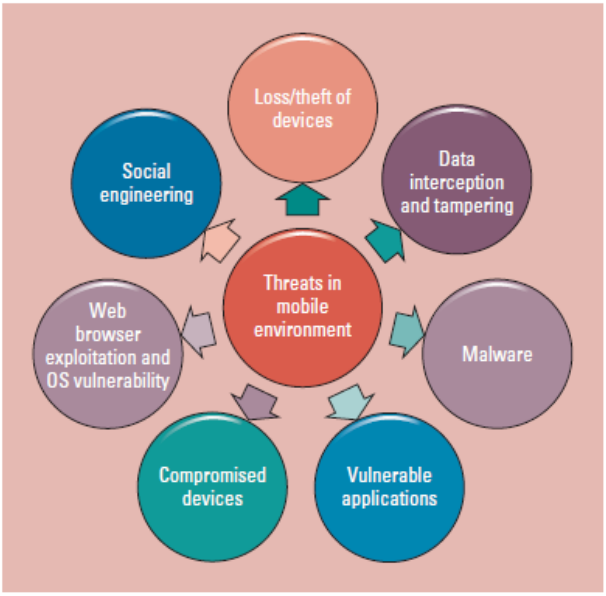


Figure 10 - Prominent threats in a mobile environment (Jain & Shanbhag, 2012)

Jailbreaking (for iOS devices) or Rooting (for Android devices) refers to the process of allowing a user to remove the logical limitations that are placed on the device, allowing the user to gain root access to, and gain more control over the device (Chaganti, S; Bayne, 2011). Though Jailbreaking & Rooting of devices is not a risk in itself because it theoretically does not directly affect the confidentiality, integrity or availability of information, it does significantly increase the likelihood or impact of other risks occurring. Should a rooted device for instance be hacked, the amount of information the hacker will potentially have access to will be much greater than if the device would not have been rooted.

There are several other studies that also identify attacks to enterprise systems, mobile enterprise systems, or mobile devices, and end up with their own list of attacks and attack types. These studies have been compared to compose a list that encompasses all identified threats that pose a risk to security of information in mobile enterprise systems. The main categories of threats include: (1) Social engineering, (2) Web exploits, (3) Code injections, (4) Encryption attacks, (5) Malware, (6) Insider attacks & errors, (7) Device vulnerabilities, (8) Technical threats, and (8) Environmental threats. A full overview of this categorization of mobile threats and their explanations is added in Apendix B: Mobile threat categorization.

3.2.2 Controls

A first step in the process towards better information security, is being aware of the various risks that have an impact on the information system (as described in section 3.2) (Rhee, Jeon, & Won, 2012). Identification of the various risks that have an impact on the information system means being able to

define and implement applicable countermeasures to mitigate these risks, so-called controls. While controls as a response to risks and attacks have traditionally been focused on identifying indicators of such events within a network, to then isolate and stop them from causing more harm (detect and correct), examination of turning points prior to the launch of an attack is much less common (Swanson, Astrich, & Robinson, 2012). This emphasizes the need for controls that also include prevention of attacks (prevent), and not just remediate a risk after it has occurred already.

Nowadays, it appears no longer to be sufficient for organizations to simply buy a bunch of tools to protect them against each mechanism of launching an attack. Although few would abandon traditional security measures such as anti-virus software, firewalls, and intrusion prevention products (as they should not), there is a fairly accepted consensus in both the business and scientific environment, that the technology to keep malicious actors at bay is not completely successful (Potts, 2012). Therefore, it is important to look at security of information as more than just a set of technological mechanisms: there are more aspects relevant when talking about securing information and controlling related risks. Freeman (2011) points this out by stating that the unique nature of information security related risks, is due to the interaction of people, processes and technology (PPT model, Figure 11). With regard to the PPT dimensions, and the 'People' dimension more specifically, Julie & Ryan (2011) state that users of IT seem to have thrown up their collective hands in the functional equivalent of: "it's not my job". It appears there is an attitude that information security is something that someone else does, i.e. employees expect that security is a service that is provided by the organization they work for.

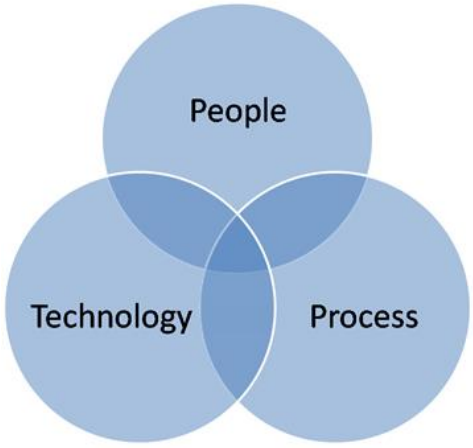


Figure 11 - PPT model

This emphasizes the interplay between the three dimensions in the PPT model; aspects in all dimensions are essential in achieving information security goals. Controls are therefore commonly referred to as the activities, processes, procedures, and mechanisms that should mitigate identified risks, and not simply a set of technical counter measures. The ISO 27000 standards defines a control as "Any administrative, managerial, technical, or legal method that is used to modify or manage information security risk" (ISO/IEC, 2007). Controls can be classified as one of three control types: (1) Preventive, (2) Detective, and (3) Corrective (Muchenje, 2012). Preventive controls are designed to prevent risks from occurring, detective controls to detect when the consequences of a risk have occurred, and corrective controls to repair the consequences of a risk, to the desirable situation. Other studies such as the SAC Report add the distinction of automated versus manual controls (Ramamoorti & Weidenmier, 2004): automated controls function continuously (no one needs to impose the need for the control), and manual controls need to be manually initiated by an actor.

The ISO 27002 standard (ISO/IEC, 2007) defines 14 aspects that should be covered in information security management:

1. Information security policies
2. Organization of information security

3. Human resources security
4. Asset management
5. Access control
6. Cryptography
7. Physical and environmental security
8. Operations security
9. Communications security
10. Systems acquisition, development and maintenance
11. Supplier relationships
12. Information security incident management
13. Information security aspects of business continuity management
14. Compliance

Each of these aspects specifies control objectives (35 in total) composed of specific controls (114 in total), accompanied with implementation guidance and, in some cases, additional explanatory notes. Controls that have to do with mobility specifically can be found occasionally throughout the standard, for instance in subsection 5.7: 'Wearable computers and teleworks'. The area considers some controls and security policies for mobile devices (such as laptops, tablet PCs, wearable ICT devices, smartphones, and USB gadgets), but does not describe such matters in consideration with the extending mobility of ERP solutions specifically, nor in great detail. ERP mobility influences many of the 14 aspects in the sense that controls may need to be altered or extended, for example the situation were an employee leaves the organization. In this case his/her access right should be updated accordingly (removed), also on possibly personally owned mobile devices. Area 3.3: 'Termination and change of employment', includes controls that address this issue: it discusses security aspects of a person's exit from the organization or significant changes of roles. With personally owned mobile devices brought into the corporate network however, the information stored on the device as well as access rights associated with the device need to be revoked also, which is not specified.

Organizational policies typically function as a general preventive measure to mitigate risks mostly involved with employees, in case of irresponsible usage in and outside the corporate environment. Successfully getting employees to comply with regulations set in policy limits the risks of blended threats, which means that employees should also get educated in the basics of potential threats (Markelj & Bernik, 2012). Policies could for instance include user awareness programs that consider guidelines on how to maintain device access codes, how to identify a secure connection, and knowledge on the defined procedures for device loss or termination of employment. Other policies could consider an offline lease policy (defining how long an app can be used without connection to the corporate network), an app update policy, jail broken policies, and data control policies (Citrix, 2013).

To complement such policies, technical measures should be implemented also. Such controls could include implementing so-called 'secure containers' that ensure a separation of private and corporate data, but also installation of security apps that are capable of securing specifics folders on a device with authentication requirements. The 800-124 special publication of NIST defines its own set of controls, specifically tailored towards mobile devices in an enterprise (Scarfone, Karen; Souppaya, 2013). The publication specifies a set of specific control activities that can be implemented to mitigate risks arising from mobility. The NOREA (Nederlandse Order van Register EDP-Auditors), which is the organization

responsible for registration of RE-Auditors in the Netherlands, also define a list of specific control activities for mobile devices brought into the enterprise. An overview of controls from both organizations can be found in Appendix C: Control overview.

3.3 Internal Controls

The pursuit of information security in an enterprise is about alleviating concerns, or in other words: mitigating risks. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines internal control as "a process, effected by an entities board, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives such as effectiveness and efficiency of operations, reliability of financial reporting, and compliance with regulation" (COSO, 2011). Without effective IT controls in place, an organization may not be able to rely on the different IT components used in the organization (Vodafone, 2010), making it a critical part of the accounting and auditing environment (Bradford et al., 2014). Guaranteeing nothing will happen is impossible, but residual risk will need to be brought to an acceptable level by implementing controls that mitigate the risks that have been identified (Freeman, 2011).

These internal controls, of which many are IT related, are tested and verified by external or internal (IT) auditors. Auditors play an important role in the process of ensuring controls are properly implemented (Debreceny, 2013). They assess and evaluate the effectiveness of internal control systems, and contribute to ongoing effectiveness (COSO, 2013; Debreceny, 2013). Put differently, they test whether or not implemented controls work as they were designed to, and report their findings back to the organization subject to the audit. In the context of information security and within this thesis, a control is defined as any administrative, managerial, technical, or legal method that is used to modify or manage information security risk (ISO/IEC, 2007). This includes practices, processes, procedures, policies, tools, and techniques, essentially anything that contributes to modifying and managing the risks affecting the confidentiality, integrity, and availability of information. While controls are often referred to simply as countermeasures, or safeguards, an organization's internal control is composed of such controls that cover the entire organizational IT infrastructure and applications (Stoel & Muhanna, 2011). With respect to an organization's internal control system, there are typically two types of controls: general IT controls and application controls.

General IT controls (commonly referred to as GITC's) cover risks associated with the IT infrastructure and environment of an organization. They are designed to ensure that an entity's control environment is well managed and applied to all sizes of systems, ranging from large mainframe systems to client/server system and laptop computer systems (Chang, Yen, Chang, & Jan, 2014). Moreover, GITC's can support application controls, which address risks that arise in the application itself, rather the IT infrastructure. An example of a general IT control is a procedure that is set by an organization, specifying how often and of what sort of data back-ups should be made.

Application controls on the other hand include input, processing, and output controls, based on the flow of data processing. They focus on the completeness, validity, and authorization of data in a specific application (Chang et al., 2014). In application controls, the IT auditor's knowledge of the intricacies of the business is as important, if not more so, as the technical knowledge (Sayana, 2013). Hence the first step in testing application controls is therefore to understand the business function/activity that the

software serves. This can for instance be done through the study of the operating/work procedures or other reference material of the organization subject to the audit, by interviewing the organization's personnel, or alternatively by inspecting the system itself to check whether or not controls are effective (Sayana, 2013). An example of an application control, in the context of an organization that issues digital certificates as a government service (PKI overheid in The Netherlands), could involve the process of determining whether or not unauthorized parties have access to the system. To be able to do so, the auditor must have an understanding of the context of the service that is delivered through the system, so the auditor can understand which parties should and which should not have access to (certain parts of) the system.

To illustrate the workings of an organization's internal control system, let us look at the following example. In the context of general threats posing a risk to information security, Rodosek & Golling (2013) map different types of attacks according to their impact on one or more of the three information security goals (confidentiality, integrity, availability). These attacks are then linked to possible countermeasures that should be implemented by an organization to mitigate the risk of such threats (Figure 12). The set of countermeasures in an organization together form the basis of an organization's internal controls, and exactly this is what is tested and evaluated by the auditor; whether or not these countermeasures are working effectively.

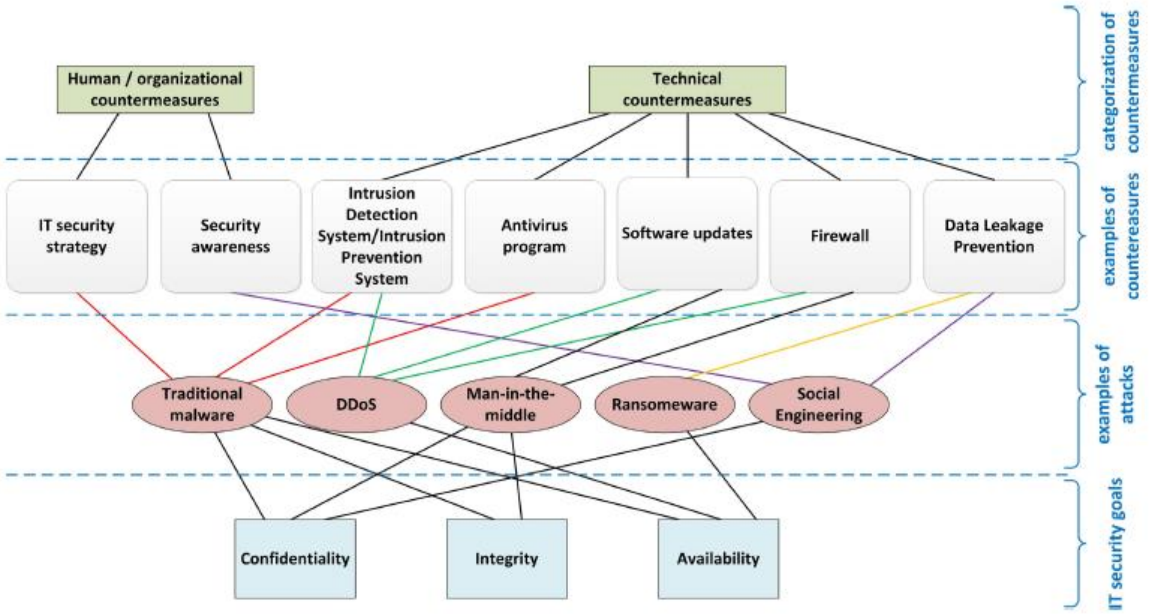


Figure 12 - Attacks on information security goals (Rodosek & Gossling, 2013)

While the approach taken by Rodosek & Golling (2013) of linking controls to, in this case threats, is similar to the approach followed in this thesis (linking controls to risks), some important elements are missing in their framework. Besides the fact that their framework is obviously not specifically tailored towards ERP mobility, one of the fundamental things is that they have only focused on intentional, technical attacks, and only from external sources. This means that risks that are either of different nature

(human), from for instance within the organization that could even occur accidently, are not accounted for. Also, where risks occur, and where and how controls should be implemented, is not discussed.

3.3.1 Known control frameworks

Several well-known frameworks exist that can be used as guidelines to test internal controls. They consist out of guidelines and control procedures that (IT) auditors can use for testing controls. Essentially, such a framework consists of two main elements: risks on the one-hand and mitigating controls on the other. Control frameworks depicts how an organization's internal control system is organized and categorized, giving insight in the entire internal control system in place, that is designed to minimize as much as possible risks affecting the organization. In other words, a control framework depicts the required elements organizations should consider to minimize their risks.

However, there is no such thing as a control framework that is usable for every audit. Each control framework has its own area of focus, and each audit could require different controls. Control frameworks and risk models must therefore be tailored to a given organizations (Stott & Parker, 2002). To provide context regarding the use of control frameworks by (IT) auditors, several well-known and renowned control frameworks that are used today day are discussed.

COSO

The COSO Report is a generally accepted accounting and auditing professional body on risk management. The COSO Internal Control-Integrated Framework is focused on the entire enterprise. It provides guidelines for public reporting on internal controls, and provides materials that management, board of directors, auditors, and other personnel can use to evaluate the internal control system within an organization. The COSO framework has two major goals (Muchenje, 2012):

- To establish a common definition of internal control that serves many different parties, and
- To provide a standard against which organizations can assess their control systems and determine how to improve them

According to COSO the framework "aids in providing assurance regarding the achievement of objectives", in three categories (Haex, Prinsenberg, & Niekus, 2014):

(1) Operations: pertain to the effectiveness and efficiency of organizational operations
(2) Reporting: pertain to the reliability of (financial) reporting, both internal and external
(3) Compliance: pertain to the adherence to laws and regulations the organization is subject to

These three main objectives can be found as entity-level objectives in an organization. These objectives flow down the hierarchy of an organization and are transformed into sub-objectives that are applicable for different organizational levels: Division, Operating unit, and Functional. The framework consists of five components to which objectives are relevant, and consider how an organization can achieve its objectives (Lindow & Race, 2002).

- Control environment: The set of standards, processes and structure that provide the basis for carrying out internal control across the organization. It comprises the integrity and ethical values of the organization and justifies the governance responsibilities.
- Risk assessment: This is the practice of identifying and assessing risks that will be encountered while achieving objectives.
- Control activities: These are the actions established through policies and procedures that ensure that the degree of risk mitigation established by the management is carried out.
- Information and communication: Information is necessary within the organization to carry out internal control responsibilities. Communication is the continuous process of providing, sharing and obtaining the information that is needed.
- Monitoring activities: This is the practice of ongoing evaluations, in order to make sure that all the five components of internal control are present and functioning well. This produces a continuous loop of feedback that is used as input to redesign and improve the functioning of the five components.

Figure 13 - COSO Internal Control-Integrated Framework (COSO, 2012)

The process of providing assurance regarding the organizational objectives is an iterative and multidirectional process (Wielstra, 2014). This means that different components in the framework influence each other, and information gained or produced in one component can serve as input for another. Figure 13 provides an overview of the objectives (X-axis), components (Y-axis), and organizational levels (Z-axis) in the COSO framework.

CobIT

COBIT is an acronym for Control Objectives for Information and related Technology, developed by the Information Systems Audit and Control (ISACA) Foundation in cooperation with the IT Governance Institute (ITGI). It is developed as a framework of generally applicable information system security and control practices for information technology control (Muchenje, 2012), and links risk management practices to business processes as well as to internal control (Pederiva, 2003; Rikhardsson, Best, Green, & Rosemann, 2006). The major concern and application of COBIT is to enable the development of unambiguous policies and best practices for IT control, industry-wide. The framework outlines platform and application independent IT control objectives, and classifies IT resources in five groups (Thurner, 2010):

- Data: numbers, text, dates, graphics, sounds)
- Application systems: sum of manual and programmed procedures
- Technology: hardware, operating systems, network equipment, etc.
- Facilities: resources used to house and support information systems
- People: individuals' skills and ability to plan, organize, acquire, deliver, support and monitor information systems and services

Accordingly with these IT resources, the COBIT framework groups IT processes that employ them into four domains (Muchenje, 2012): (1) Planning and organization, (2) Acquisition and implementation, (3) Delivery and support, and (4) Monitoring and evaluation. Essentially, the framework provides high level control statements for these IT processes. It identifies the business need satisfied by the control statement, identifies the IT resources managed by specific processes, states the enabling controls, and list major applicable control objectives (Muchenje, 2012).

SAC report & eSAC model

The electronic Systems Assurance and Controls (eSAC) model was issued in 2001, and is an adaptation of the System Auditability and Control (SAC) Report issued in 1977 (Ramamoorti & Weidenmier, 2004). Both were drafted by the Institute of Internal Auditors (IIA) Research Foundation. The SAC report defines the system of internal control, describes its components, and provides several classifications of controls. Moreover, it describes control objectives and risks, and defines the role of the internal auditor. The main purpose of the SAC Report is to provide guidance on using, managing, and protecting information technology resources, similar to COBIT. It also discusses the effects of end-user computing, telecommunication, and emerging technologies. It classifies internal controls in information systems in five categories:

- Preventive, detective, and corrective (when)
- Discretionary and non-discretionary (how)
- Voluntary and mandated (can it be circumvented)
- Manual and automated (who imposes the need)
- Application and general (where)

Based on the SAC report, the eSAC model (Figure 14) was developed to facilitate discussion in relating issues. It was designed because "internal auditors must understand the business risks resulting from changes in technology, be able to articulate responsive risk management strategies to management, and provide assurance on the availability, capability, functionality, protectability, accountability, and auditability of the systems involved" (Stott & Parker, 2002).

The eSAC model has one central element: an organization's internal control system. This system is derived from an organization's mission, values, strategies, and objectives, and in turn leads to improved business results reputation, and learning. Two main factors influence this input-processing-output process: markets forces and velocity (e.g. customer demands, regulations, etc.), and external interdependencies (providers, partners, etc.). All in all, and organization's internal control system functions in a dynamic environment that is constantly changing. Because of this, it need to be monitored and improved on a continuous basis, so that new and amplified risks (for instance emerging from new technologies) are mitigated.

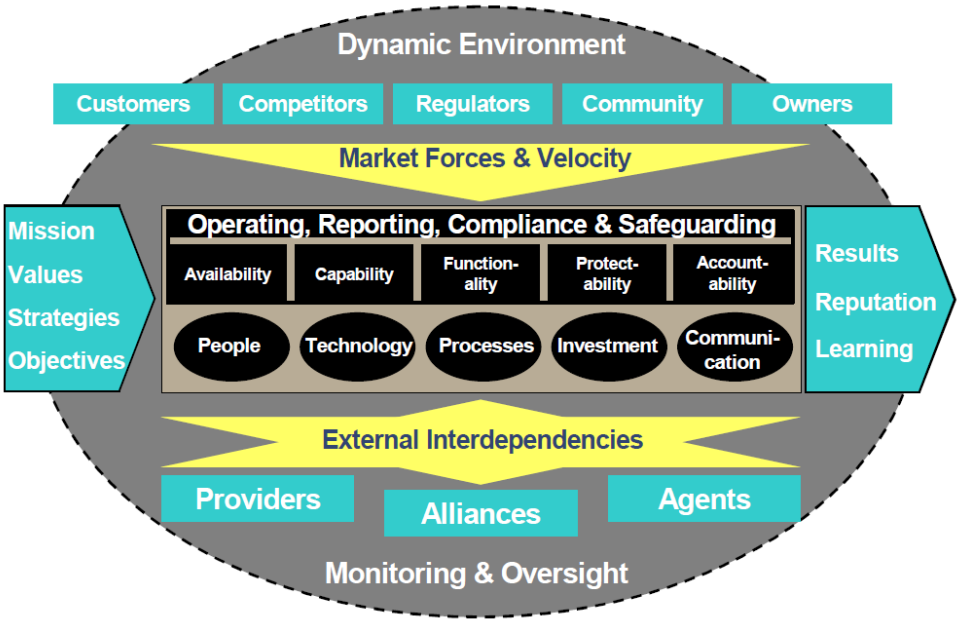


Figure 14 - eSAC model (IIA, 2002)

Contents of the eSAC model are, aside from the SAC report, largely based on the COSO framework. Control objectives in an organization's internal control system as defined in COSO are for instance depicted in the center of the framework (Operating, Reporting & Compliance & Safeguarding), which are further decomposed in 'Assurance objectives' that need to be achieved in the row below those (Availability, Capability, Functionality, Protectability, and Accountability). Achieving these assurance objectives requires an adequate infrastructure, resources, and organizational commitment (Stott & Parker, 2002) based on areas like people, process and technology, but also investment and communication.

ISO 27000

The International Organization for Standardization (ISO) has developed more than 16,000 international standards for several stakeholders. The ISO 27000 series helps organizations establish information security standards that meet business needs while ensuring compliance with regulatory and contractual requirements. While the ISO 27001 specification considers an information security management system, ISO 27002 represents the standard that outlines numerous controls that can be implemented. Furthermore, a categorization is made for information assets that distinguishing four categories: Pure information assets, Physical IT assets, IT service assets, and Human information assets. A complete overview including descriptions of each asset type can be found in appendix A. The ISO 27005 standard provides a number of examples of threats and vulnerabilities that could pose a risk and affect one or more of the information security goals described in section 3.2. Furthermore it provides a high level approach to risk management.

Altogether, the ISO 27000 series provides different standards for Information Technology, Information Security, and Information Security Management Systems (Janssen, 2013). The ISO 27000 series consists of 9 specific standards, each with its own area of focus (ISO/IEC 27000, 2009):

- ISO/IEC 27000:2009, Information Security Management Systems – Overview and vocabulary
- ISO/IEC 27001:2005, Information Security Management Systems – Requirements

- ISO/IEC 27002:2005, Code of practice for information security management
- ISO/IEC 27003, Information Security Management Systems implementation guidance
- ISO/IEC 27004, Information Security Management: Measurement
- ISO/IEC 27005:2008, Information security risk management
- ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007, Guidelines for information security management systems auditing
- ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

Framework for Internal Control Systems

In 1998 the Basle Committee on Banking Supervision introduced a framework for the evaluation of internal control systems. While originally focused on financial banking institutions, many principles are related and relevant. The framework describes the essential elements to a sound internal control system, in terms of five basic principles (Basle Committee on Banking Supervision, 1998): (1) management oversight and control culture, (2) risk recognition and assessment, (3) control activities and segregation of duties, (4) information and communication, and (5) monitoring activities and correcting deficiencies. Effective functioning of these five elements is key to an organization achieving its performance, information, and compliance objectives. Elements (2), (3), and (5) are especially interesting for this research, since they involve the process of assessing and controlling an organization's risks, and most importantly monitoring and correcting deficiencies (i.e. testing controls in terms of their effectiveness).

Control activities should include top level reviews, appropriate controls for different departments or divisions (also physical controls), checking for compliance and follow-up on non-compliance issues, a system of approvals and authorizations, and a system of verification and reconciliation (Basle Committee on Banking Supervision, 1998). The framework describes that controls not only need to be in place, but that the operational effectiveness of controls need to be tested as well. Emphasized is the need for verification of controls, which is an activity performed by the auditor. If we for instance consider the control statement: "employees who leave the organization must have their access right removed". In this case the auditor will not only need to check whether this particular procedure exists in the organization, more importantly the auditor will have to test whether this procedure is actually lived by in practice.

3.3.2 IT Auditing

The generic information security risk management process follows three steps: (1) Risk assessment, (2) Risk treatment and (3) Residual risk (ISO/IEC 27005, 2008). On a more detailed level, the risk assessment step again includes three steps: (1) Risk identification, (2) Risk analysis, and (3) Risk evaluation (ISO 31000, 2009). As a result of the risk assessment phase, a plan can be produced that depicts the risks in a particular organization. Typically this also involves quantification of risks in terms of their impact and likelihood, as described in section 3.2.1.

Based on a risk evaluation of the assessment a suitable risk treatment can be determined, which is a plan that specifies which controls need to be implemented. Which controls will or will not me implemented is a decision each organization will have to make for itself. This decision is a weigh-off between the amount of risk that will be mitigated on the one hand, and the costs of implementing the necessary controls on the other, as also stated by one of the interviewees (E01). Once this decision has been made, and a treatment

plan is agreed upon, applicable controls will have to be implemented. These controls are implemented inside the organization. The combined set of controls in an organization is referred to as the organization's internal control system, which protects the organization from all kinds of risks, ranging from employees stealing confidential corporate data to cybercriminals trying to hack into enterprise systems.

This is where the role of the IT auditor comes into play. To check whether or not internal controls do what they were designed to do, they need to be tested to see if they are actually effective. To do this, IT auditors test an organization's internal controls using so-called risk-control frameworks. Such frameworks provide the IT auditor an overview of the risks applicable in the context of the audit, the control areas that are relevant including specific controls in these areas, and usually also procedures that describe how the controls need to be tested.

Based on the results of an audit, i.e. the results of testing the effectiveness of controls, the organization may choose to initiate actions to improve their internal controls. Internal controls may then need to be revised to appropriately address any new or previously uncontrolled risks (Basle Committee on Banking Supervision, 1998). As an example, a control can be defined as followed: "mobile operating system versions are continuously monitored and updated by the IT department". Should an auditor test this control and discover that such a process is not in place, the result of that test may be "ineffective". The organization may then decide to improve that control so it actually mitigates the risk(s) it was supposed to, i.e. implement a process that actually monitors and updates operating system versions. Alternatively, the organization may simply choose not to, depending on their weighing of priorities (mitigating risks versus spending money).

In essence, delivering the results of testing controls concludes the process of an IT audit, which means that the responsibility of actually improving internal controls still lies with management of the client subject to the audit. In light of the broader risk management process, the IT audit can essentially be seen as a check in a continuous improvement cycle, where risks keep getting assessed, and after each assessment a decision has to be made on which controls will (or will not) be implemented or improved. This process can therefore be mapped to the Plan-Do-Check-Act (PDCA) cycle, also known as the Deming Cycle due to its creator, which represents the continuous improvement aspect of quality management (Gidey, Jilcha, Beshah, & Kitaw, 2014). Figure 15 depicts the IT audit process mapped to the PDCA cycle.

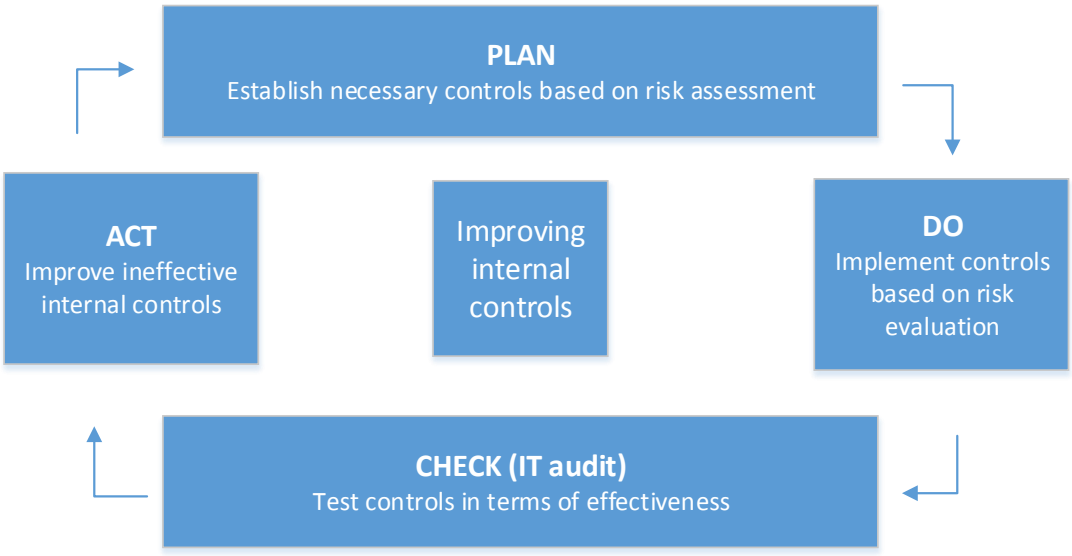


Figure 15 - IT audit process mapped to the PDCA cycle

3.4 Risk areas

The occurrence of a risk is based on two causing factors (threats and vulnerabilities) and broken down into two components (impact and likelihood) as described in section 3.2.1. The level at which risks are discussed in literature however differ a lot, some refer to risks when discussing specific threats while others do so vice versa. Both are taken into account, and this section elaborates on the areas that are of relevance in which these risks can be categorized.

The well-known People, Process and Technology categorization (as described in section 3.2.2) defines three areas that are relevant to general information security. While still valid, a more detailed distinction of areas is desirable. Threats and risks related to mobility have been classified on a more detailed level in several studies, for instance risk associated with the user of mobile devices as the category "user", or risks associated with the device itself as the category "device". All of these areas however can ultimately be mapped accordingly with the PPT dimensions. For instance, the category "user" would fall in the People dimension, and the category "device" would fall in the Technology dimension.

Janssen (2013), defines seven attention areas that need to be taken into account with enterprise mobility (Figure 16). These areas were defined in the broader context of enterprise mobility, which is considered as the "collective term for all activities that are linked to using mobile devices in large businesses, including activities that are not directly part of mobile applications as organizational activities and facility management" (Janssen, 2013, pp. 9). Though the scope of this thesis is focused on the impact of mobility as an extension to traditional ERP solutions, thus narrowing mobile usage down to the usage of mobile enterprise applications in combination with data stored in a back-end enterprise system, the areas do provide a solid base of relevant areas upon which the work in this thesis can build on.

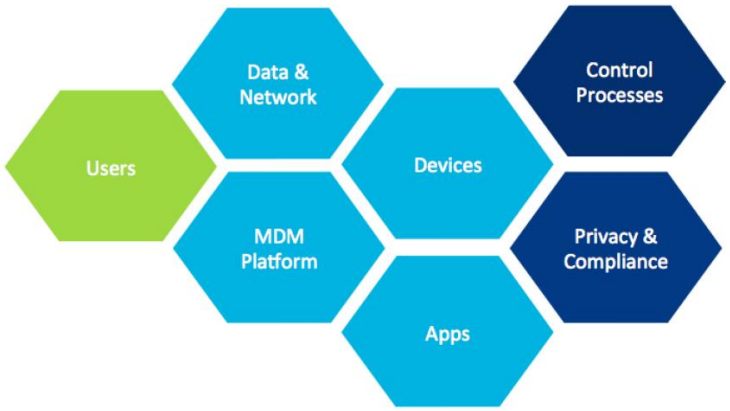


Figure 16 - Enterprise Mobility Attention Areas (Janssen, 2013)

These areas are also mapped accordingly with the PPT dimensions. The green area ("User") represents the People dimension, whereas the light-blue areas represents the Technology dimension, and the dark-blue areas the Process dimension. Each area is explained below.

- **Users:** threats that are initiated by the people who use the mobile devices, and mitigating controls that are appointed to positively influence the user on their mobile usage
- **Privacy & Compliance:** threats that can violate the privacy of employees, threats that can lead to consequences to the organization for not being compliant with (inter)national legislation on privacy, encryption, or other mobile device related laws, and controls that prevent these violations
- **Devices:** vulnerabilities on the physical hardware and operating system of the mobile device, and control based on that
- **MDM platform:** vulnerabilities found in systems that manage mobile devices (MDM) and systems that enable services that are used on mobile devices, as well as controls that mitigate them on platform level
- **Apps:** vulnerabilities found in any app (self-developed or third party) running on the mobile device, and controls that mitigate such vulnerabilities
- **Data & Network:** all threats directly related to the exposure or loss of enterprise data (via any mobile network connection, and controls that mitigate the possibility of data exposure/loss
- **Control processes:** contains all threats that are opposed by organizational processes that are not (efficiently) arranged to manage the use of mobile devices

Fibikova & Mueller (2012) define four information security areas that need to be taken into account when implementing information security, and thus where risks need to be mitigated: Information users, Business processes, Applications, and Infrastructure. The four information security areas in this study are again closely related to information security in M-ERP solutions, and relate to some extent to the areas defined by Janssen. Though the areas "Information users", "Business process", and "Applications" areas correspond to the "User", "Control processes", and "Apps" areas respectively, they are tailored towards the more general concept of securing information in an enterprise. The "Infrastructure" area for instance is a broader term encompassing several areas from Janssen: "Data & Network", "MDM platform", and "Devices", an area depicted by Fibikova & Mueller (2012) as "how well does the infrastructure provide capabilities to protect information against unauthorized access and modification".

In addition though, Fibikova & Mueller (2012) state that the combined set of measures (i.e. controls) that are implemented to ensure security of information in such areas, need to adhere to five principles: (1) they needs to cover all four information security areas (completeness), (2) provide adequate protection of information (effectiveness), (3) be seamlessly integrated into the processes (integration), (4) be supported by efficient tools and simple templates (support), and (5) need to avoid putting an unacceptable burden on employees (simplicity). Three of these principles are especially important in the development of the M-ERP risk-control framework. It is important that the framework will be complete in terms of considering all relevant areas (completeness), specific controls should be effective in providing protection of information (effectiveness), and controls should be integrated with operational processes and procedures as much as possible (integration).

The relation among the different areas, as well as to information in general, is depicted in Figure 17. In essence the cycle starts with the user of a system, i.e. employees creating, processing, and using data for their day-to-day working activities. These users process and create information to jointly execute certain business processes. Such business processes can thus be seen as a group of information users who work create, process and use information. To actually do this however, business processes are supported with applications. These application in turn run on a defined IT infrastructure, on which all information in the organization is hosted upon, completing the cycle.

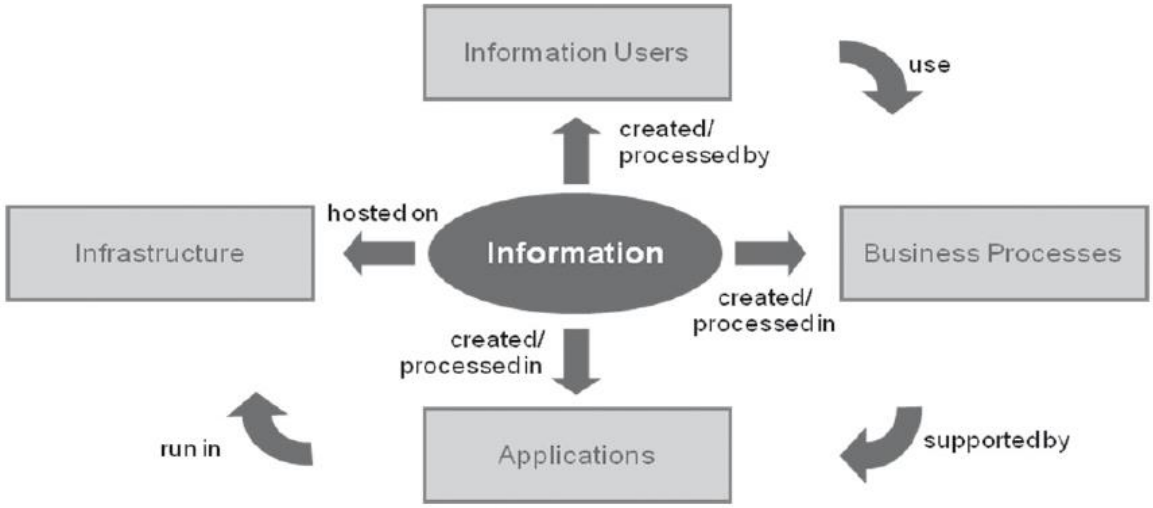


Figure 17 - Information processing in an enterprise environment (Fibikova & Mueller, 2012)

An SAP report from 2013 (SAP, 2013) elaborates further on the technological areas in Figures 16 and 17. They define two more elements in their own SAP ERP mobile platform besides Application security and Platform (Infrastructure) security: **Transport security**, and **Device security**. Transport security involves securing information flows throughout the entire system that are processed over networks, corresponding with the "Data & Network" area of Janssen. Device security considers securing information and access to the mobile device accessing the system, corresponding to the "Device" area. These security elements are however solely focused from a system's perspective, hence they do not cover the full scope of the impact mobility has on ERP environments. While relevant, the elements are merely focused on the 'Technology' dimension, and do not consider aspects regarding the 'People' or 'Processes' dimensions (though not surprisingly, since SAP would solely be focused on securing their product).

The NCSC (Nationaal Cyber Security Centrum), which is the national cyber security center in the Netherlands, also considers the areas User, Network (Transport security), Databases & Platform, Device access, and Application as important (NCSC, 2012a, 2012b). They do however add one more area: **Policy.** This area considers a general policy set by the organization that includes minimum preconditions (organization-wide) and more specific policy applicable to mobile devices that should help avoid and thus mitigate potential risks. Also notable is the difference in interpretation of the 'Device' area. The NCSC's approach is from a user access point of view (logical and physical access), including identity and access management. Other studies tend to consider this area from a much wider perspective, also for instance discussing activities that take place on the device: flaws in mobile operating systems, physical hardware flaws, and installation of third-party apps.

The 800-124 special publication of NIST (National Institute of Standards and Technology) defines their own seven high-level areas in which threats and vulnerabilities take place (Scarfone, Karen; Souppaya, 2013). These areas are primarily focused on securing the mobile device in an enterprise, and do not consider other components in the infrastructure of a M-ERP environment. In other words, they consider information security from a mobile device security perspective, which is merely the end-point of a M-ERP solution. These areas thus further elaborate on the "Device" attention area as it was defined by other studies such as Jansen and the NCSC, though implicitly mentioning other areas too (Network, Applications).

- **Lack of physical security controls:** organizations should assume mobile devices will get lost or stolen. Mitigation consists of three layers; (1) authentication before gaining access, (2) encryption, and (3) user training and awareness
- **Use of untrusted mobile devices:** organizations should assume that all mobile devices are untrusted, unless it has been properly secured and it is being monitored while in use with enterprise applications or data
- **Use of untrusted networks:** organizations normally have no control over external networks, and mobile device security should be planned on assumption that networks between the device and the organization cannot be trusted
- **Use of untrusted applications:** organizations should plan their mobile device security on the assumption that unknown third-party mobile device applications should not be trusted
- **Interaction with other systems:** mobile devices may interact with other systems in terms of data exchange (including synchronization), by connecting with a laptop or desktop wirelessly or via a cable
- **Use of untrusted content:** mobile devices may use content other devices typically do not encounter, such as QR-codes.
- **Use of location services:** enable targeted attacks because it is easier for potential attackers to determine where the user and the mobile device are, and to correlate that information with other sources about who the user associates with and the kinds of activities they perform in particular locations

3.4.1 Preliminary areas

To summarize, all mentioned areas have been analyzed for applicability in the context of ERP mobility, and have been grouped together. There have been many studies either focusing on securing the mobile device in an enterprise, or focusing on general information security areas. Studies investigating the impact

of mobility when integrated with back-end ERP systems, are lacking. Nonetheless the attention areas provided so far are closely related, and provide a first set of areas that are relevant in ERP mobility environments, where risks could occur. An overview of areas is presented in Table 6. Together they cover the entire scope of ERP mobility, so that risks associated with M-ERP environments can be categorized in one of the 11 areas, as well as specific control activities that mitigate these risks.

No.	Area	Jansen	F&M	SAP	NCSC	NIST
1	User	✓	✓		✓	
2	Privacy & Compliance	✓				
3	Device (access)	✓		✓	✓	✓
4	Mobile platform	✓		✓	✓	
5	Apps	✓	✓	✓	✓	✓
6	Data & Network	✓		✓	✓	✓
7	Control processes	✓	✓			
8	Infrastructure		✓			
9	DMZ security			✓		
10	Policy				✓	
11	System interaction					✓

Table 6 - Preliminary areas

The area "Infrastructure essentially encompasses the entire IT infrastructure supporting a M-ERP system. This means that the area would include several other attention areas, such as 'Mobile platform', 'DMZ security', 'Device', and possibly even 'Data & Network'. The scope of the 'Infrastructure' area is thus on a higher level that the other areas, and it is represented by several other more specific areas combined. This area is therefore omitted from the list.

The area 'DMZ security' was only mentioned by one source. While relevant, it is considered part of the network-aspect in the 'Data & Network' area. The 'DMZ security' area is therefore not included on its own but considered as part of the 'Data & Network' area.

Furthermore, the area 'Privacy & Compliance' has been omitted. Though very interesting and relevant, issues related specifically to privacy and/or compliance issues pose a research area in their own. As explained in chapter 1.4, such aspects would not be in the scope of this thesis.

The analysis process resulted in 8 preliminary risk areas that can be mapped against the PPT model and its three dimensions, depicted in the final categorization of areas presented in Figure 18. The bottom areas in yellow correspond with the underlying technology that supports usage of mobile device (Technology). The middle areas in green correspond with the processes, procedures, and policies that relate to the technology (Process dimension). The blue area on top finally relates to the user of the mobile device; the employee (People dimension). Brief descriptions of each area are given below.

User

Considers all aspects related to the users who access the ERP system through their mobile device. This includes risks due to employees purposely trying to bypass security controls for personal gain, but also irresponsible mobile device usage behavior and external attacks targeted at employees such as social engineering.

Control processes and procedures

Procedures and processes defined by the organization that help ensure establishment of company policy related to ERP mobility.

Policy

Considers all aspects related to specific policy set by an organization that influences its internal control system related to ERP mobility.

Data & network

Considers all aspects related to the use of (mobile) network connections as well as the corporate network, and loss or exposure of data via these networks. This involves risks to the data itself that accessed and stored on mobile devices, as well as the network over which this data is being transmitted.

Apps

Considers all aspects related to applications installed on the mobile device, including third-party applications aside from the MEAs connecting the device to the ERP system.

Mobile platform

Considers all aspects related to the underlying platform connecting mobile devices to the back-end ERP system, representing the role of mediator and integrator, such as mobile device and mobile asset management. The mobile platform encompasses all components residing between the mobile device and back-end application.

Device

Considers all aspects related to the operating system and hardware of the mobile device used to access an ERP application, as well as physical and logical access to the device. This includes flaws, changes, and updates to the mobile operating systems, (security) configuration issues of the mobile device, as well as risks due to possible differences in the mobile devices being used by employees (especially in BYOD environments).

Environment

Considers the event where the mobile device interacts with other systems than the back-end ERP system in terms of data exchange. This could for instance be a mobile device that connects with a laptop or desktop computer and back-up data stored on the mobile device.

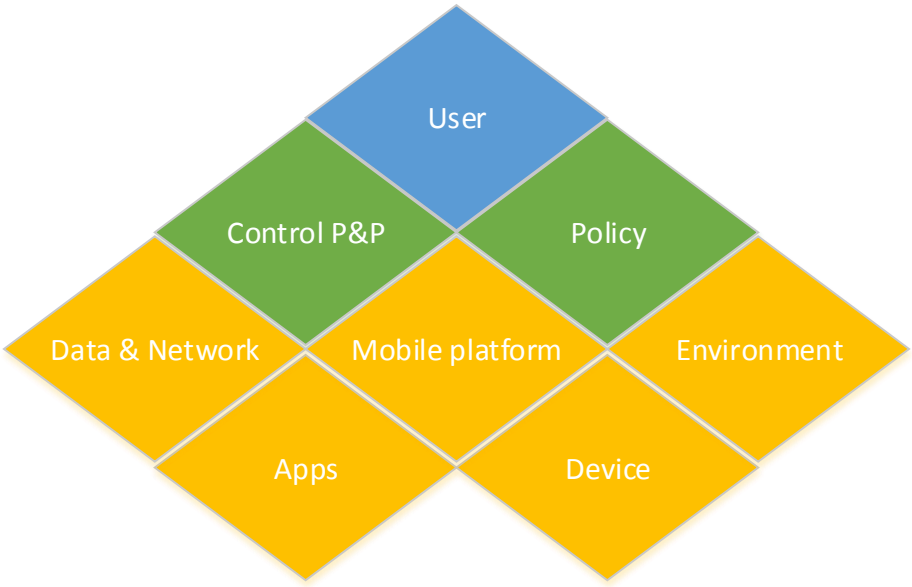


Figure 18 – Risk areas

3.5 Research gap

Based on changes in ERP systems due to mobility (its infrastructure, mobile enterprise applications, and accordingly the approach of (information) security), IT control frameworks need to be revised and extended. Currently, no comprehensive IT control frameworks exists incorporating the relevant risks that arise from mobility in ERP systems. This means that from an audit perspective, internal controls related to ERP mobility cannot be properly tested and evaluated on their effectiveness, simply because that insight is lacking. This creates a clear gap between immature (information) security measures in ERP environments extended with mobility, and mature IT risk-control frameworks used by auditors to audit ERP systems.

Chapter 4 will describe a conceptual model of the proposed control framework. A number of risk areas have been defined that are expected to cover important areas in M-ERP environments where risks could potentially occur. Weaknesses may be found in one area, which could be compensated for by a strong control in another area. It is the responsibility of the IT auditor to report on all of these findings.

Based on the risk-control framework a Risk-Control dashboard is therefore developed, one that includes the different areas defined in the control framework. The dashboard provides IT auditors the means to provide insight in the state of effectiveness of specific controls in each of the defined areas, helping IT auditors and their clients to easily determine which areas are evaluated to be weak, and which are considered strong. This also allows for backward-traceability to specific controls within each area that represent the underlying causes for that area to be considered weak or strong. Based on the conceptual model (chapter 4) and expert interviews (chapter 5), in chapter 6 a complete control framework will be presented.

4 Conceptual model

This chapter describes the main elements that have been discussed in chapter 3, that together represent the main components of the M-ERP control framework.

4.1 Relevant elements

Five distinct components are defined to together form the basis for the risk-control framework: Risks (section 3.2.1), Control objectives, Risk areas (section 3.4), Controls (section 3.2.2), and Procedures. The concepts of Risk, Control, and Risk area have been discussed extensively in the aforementioned sections of chapter 3, and constitute the three essential pillars of the risk-control framework: there are (1) risks arising from mobility to organizations of which related ones can be grouped into (2) risk attention areas, whereas risks are ultimately mitigated by specific (3) controls.

There is however no clear consensus in literature on the definition of a risk, causing the level at which risks are defined to differ a lot among different studies. Some studies refer to risks when discussing specific threats or vulnerabilities, while others refer to threats when discussing a particular risk. The concept of a risk is therefore broken down into the product of a threat and a vulnerability, as described in section 3.6. This way risks can be defined in a uniform way.

Besides risks, controls, and risk areas, two additional concepts are now added to the risk-control framework: the Control objective and the Procedure. Figure 19 depicts the relationships between the five components.

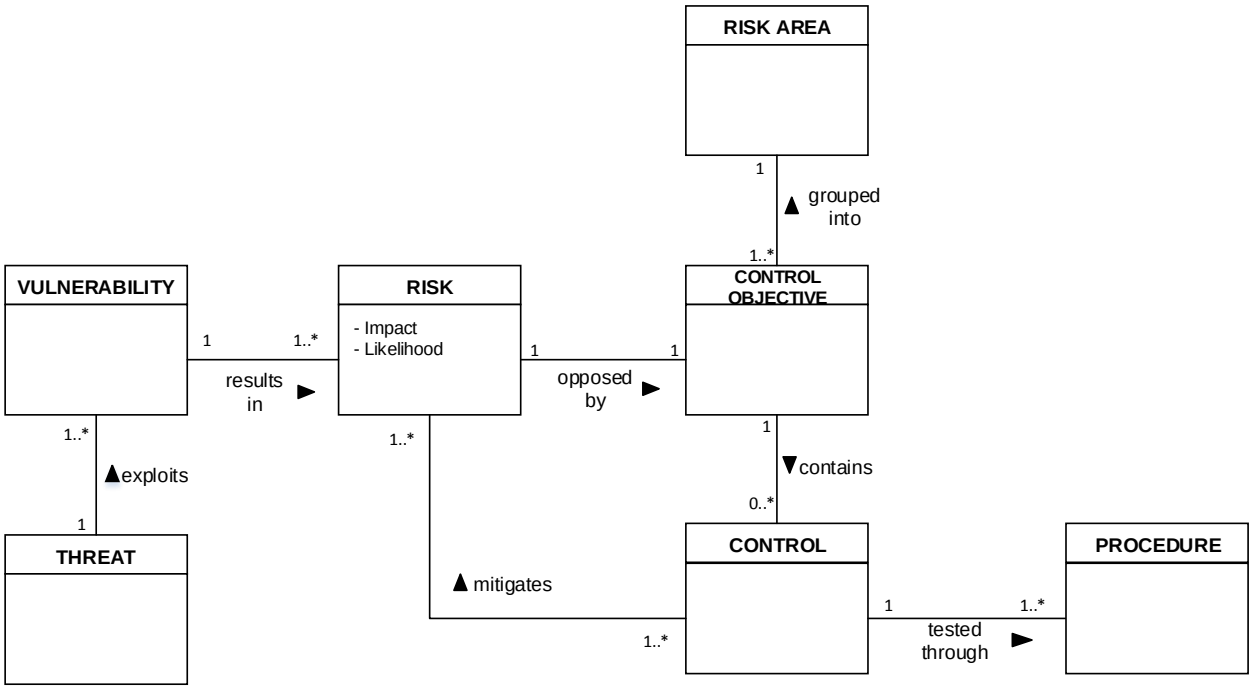


Figure 19 – Relevant elements to M-ERP risks

4.1.1 Control objective & Procedure

Control objectives are considered as the goal that organizations want to achieve with implementing (a set of) specific controls. The term is used in the CobiT framework, ISO 27000 series, as well as the eSAC

model, all described in chapter 3.6.2. Essentially, a control objective can be considered as an "anti-risk", or "1/Risk", in the sense that the objective of a set of controls is always to mitigate the risk it is addressing. As an example, a control objective can be defined as "Data is backed up on a regular basis", to mitigate the risk of losing data due to irregular back-up of data. A Control objective typically has 5 properties: "Name", "Description", "C", "I", and "A". The name of the control objective could be defined as *Data back-up*, whereas the description includes a short explanation of the goal that is to be achieved. The properties 'C', 'I', and 'A', represent the nature of the risk the control objective is addressing. They can be used to depict how the control objective is designed to achieve prevalence of one or more of the information security goals discussed in section 3.2; Confidentiality, Integrity, and Availability.

The risk of losing data due to irregular back-up (and thus its accompanying control objective) apparently has something to do with data, along with a number of others risks (for instance the risk of backup media getting stolen, damaged, or otherwise compromised, causing loss of, or changes to back-up data). These risks and control objectives can therefore be grouped together in an applicable area, in this case the 'Data & Network' area, representing the Risk attention area component. For each of the risks in this area, one or more controls should be identified. Following the example above, such a control might then be defined as: *Data is backed up on a regular basis according to an established schedule and frequency*. To summarize, these four components can now be identified:

- **Risk:** Data loss due to irregular back-ups of data
- **Risk attention area:** Data & Network
- **Control objective:** Data is backed up on a regular basis
- **Control:** Data is backed up on a regular basis according to an established schedule and frequency

According to these defined elements, this in essence means that should an organization have an established schedule and frequency in place according to which data is indeed backed up, the aforementioned risk of losing data due to irregular back-up of data is considered to be effectively mitigated, and thus the objective "Data is backed up on a regular basis" is achieved. However, for an IT auditor to test the effectiveness of this control, the auditor will not only need to determine whether there is indeed an established schedule and frequency according to which data is backed up, but also verify that backups are indeed performed according to the schedule and frequency the organization has defined. Determining there is such a plan is the first step, determining the organization actually lives by it is another.

The auditor thus won't only be checking if a control is present in the internal controls system of an organization, it will test whether that control is actually performing effectively in practice. To do this, a so-called Procedure is defined, elaborating on the steps that should be taken by the auditor to test a particular control in terms of its effectiveness. An approach to testing the effectiveness of the data back-up control for instance could include the following steps, representing the Procedure component in the framework:

1. Check if there is a documented back-up plan defining a back-up schedule or frequency
2. Check if the backup was performed on schedule, as defined in the back-up plan
3. Check if the backup ended in a success

4. Check whether when errors were encountered during back-ups, documentation was present to identify corrective actions to obtain a successful backup

After having tested the control by checking these four steps, the auditor can finally determine whether the control is operating effectively or not, and then report findings back to the client. The act of reporting back to the client finalized the audit, and marks the end of the third step in the Risk Management process as depicted in the PDCA cycle in Figure 15.

4.2 Initial concept

Based on findings from the literature study and other business reports, the risk-control framework can be filled with an initial overview of risks and applicable controls. Control objectives are grouped into the risk attention areas defined in section 3.6. For each control objective a number of applicable controls are identified, so that each of the risks can be mitigated.

Table 7 presents an overview of the initial Risk-Control framework, which is also used as a basis for discussion with for the conducted expert interviews. For the sake of readability and to facilitate discussion, only the risk areas have been included. Other components (Risk, Control objective, Control & Procedure) are shown for clarity, but not explicitly presented in detail in the framework.

Risk	Risk area		Control objective	Mitigating control	Procedure
	Name	**Dimension**			
	User	People			
	Control P&P	Process			
	Policy	Process			
	Data & Network	Technology			
	Apps	Technology			
	Mobile platform	Technology			
	Device	Technology			
	Environment	Technology			

Table 7 - Initial concept Risk-Control Framework

A preliminary version of the Risk-Control framework that incorporates different specific risks and controls that have been found from the SLR and other business reports (all discussed in chapter 3) can be found in Appendix E.

5 Empirical findings

Empirical research is used to validate or evaluate statements, proposals, or hypothesis that have been made (Peersman, 2012) . To verify the problem statement of this thesis as defined in section 1.2 Problem statement & Research Objective, and answer the research questions in section 1.3 Research Questions, several experts in the corporate field of ERP mobility have been interviewed. Interviews have been conducted following the method described in section 2.4, and the interview protocols that have been used to guide the interviews can be found in Appendix D.

5.1 Interview criteria

Interviewees with whom interviews have been conducted for this thesis can be divided in three groups: (1) Suppliers of M-ERP solutions (SUP), (2) Organizations using a M-ERP solution (ORG), and (3) Consultants or security experts helping organizations from group 2 in implementing and using the solutions offered by those in group 1 (EXP). These three groups of experts together capture the parties involved with ERP mobility.

The suppliers group (Table 8) represents experts working in organizations that develop an ERP solution, extended with mobility. This includes experts regarding M-ERP in general and M-ERP security. Interviews are conducted with experts regarding several ERP products that are being used by organizations in the Netherlands, both from a range of different suppliers. Three suppliers have been selected for interview; two relatively large ERP suppliers with their main market in the Netherlands (SUP01 & SUP 02), and one ERP supplier who is one of the market leaders on a global level (SUP03). These organizations differ a lot in size, so that insight in the maturity of these different products is also gained.

ID	Size	Interviewee role	Scope
SUP01	~ 300	Product manager ERP	Primarily the Netherlands
SUP02	~ 1700	Director Product Marketing	Primarily the Netherlands
SUP03	~ 120.000	Consultant ERP	Global

Table 8 - ERP suppliers

The second group (Table 9) represents experts working in organizations who have adopted and use a M-ERP solution in their organization, to support their day-to-day business activities for certain processes. This may include any type of organization who has adopted a form of mobility as extension to a back-end application. In addition to these interviews that were conducted to construct the M-ERP control framework, the client-expert was asked to participate in a case study to validate the M-ERP control framework (described in chapter 6) in practice.

ID	Size	Industry	Process supported with mobility
ORG01	100.000+	Governmental	Human Resources

Table 9 – Organizations using a form of ERP mobility

The consultants group (Table 10) represents experts who work at a third-party consultancy firm that helps other organizations in implementing and managing a M-ERP solution. Experts in this group vary from (mobile) security experts to general ERP platform experts, SAP and Oracle most notably. Experts from

different organizations, sizes, and roles are chosen, so that insight is gained from different ERP mobility projects.

ID	Experience	Interviewee role	Organization
EXP01	6+ years	Manager Mobile Security	Deloitte Risk Services
EXP02	10+ years	Director ERP Risk	Deloitte Risk Services
EXP03	6+ years	Manager Oracle Mobile	Deloitte Consulting
EXP04	3+ years	Manager Mobile Security	Ernst & Young
EXP05	10+	Director SAP implementations	Acorel

Table 10 - (mobile) ERP consultants

5.2 Interview results

This section elaborates on findings from the interviews that are relevant to the risk-control framework and its broader context. Discussed topics can roughly be divided into four distinct topics: ERP mobility usage from a functional perspective, connectivity of devices with the back-end application, the broader ERP mobility strategy, and associated risks and controls. Interviewees were asked questions divided in five main categories:

- **Strategy**: Interviewees were asked about their view on integrating mobile devices with ERP systems, and how this has evolved over time. This way a better understanding of the broader concept of ERP mobility is gained as well as where the market seems to be going.
- **ERP mobility usage**: Interviewees were asked for what purposes mobile devices are mainly used and what sort of processes are typically supported through mobility. This further elaborates on the broader mobile strategy, and gives an understanding of the specific context in which mobile devices operate as an extension to ERP systems. Depending on the type of supported processes and purposes, different risks may play part.
- **Connectivity**: The unique aspect of EPR mobility has to do with the connection between mobile devices and back-end applications, making this connection of great importance. Employees were asked about how mobile devices are typically connected to back-end applications, and how this is secured.
- **Risks**: Posing risks as a result from integrating mobile devices with ERP systems are then discussed, taking into account the connectivity issues, mobility usage, and overall strategies discussed earlier. A concept of the Risk-Control framework as proposed in Table 7 and Appendix F are presented to validate initial findings, as well as provide guidance for discussing relevant risks.
- **Controls**: Based on the risks that have been covered relevant and important controls are then attempted to be identified. The interviewee is also asked directly to name important controls, in case important risks were missed.

Strategy

Interviewees were asked on their broader vision of the evolution and future of ERP mobility. There was a general consensus that adoption of ERP mobility is still quite low, and the general conception of many organizations is that mobile extension of ERP solutions is a ‘nice-to-have’ instead of a necessity.

[SUP01] “Our vision and mobile strategy is in that of ‘Project Self Service’, in the sense that employees should be able to work on projects with colleagues, partners, and clients, no matter the location, time, or

device. Though we still wonder if everything should be mobile, the iPad has the capabilities to do so due to its size and hardware, and for us the iPad is considered as 'hard business' for mobility. Smaller devices such as smartphones tend to provide a less pleasant user experience in certain occasions. This could for instance result in more typos, which could mean an employee will have to redo some input, which costs time and ultimately might stop the employee from using the app."

[SUP02] "A first trend is that back-end application views have been tailored towards mobile devices, to make them more usable. It is not necessarily the case that specific new apps have been developed. A second trend is implementation of the mobile development platform, in which case the ERP supplier only delivers the middleware on which a customer can build its own apps. The third and last trend is that of native apps being developed. In this case end-users only have to download an app and register a link to their back-end application, which for instance could be based on usage of licenses per user. Overall, there are not that much organizations really committing to ERP mobility, because it simply has less priority compared to other things. Moreover, adopting mobility does not directly create business or value, making mobility for many organizations a nice-to-have instead of a necessity. Part of adopting mobility is also about showing you are a modern organization, especially when you are a large organization. New hires grow up with mobile devices, and expect no less of their employees."

[SUP03] "We bring apps on the market based on employee roles that already exist in the back-end system. An employee who owns the role of 'service employee' for which he needs to visit clients to fix certain hardware for instance could use an app specifically tailored towards the needs of his function. Many organizations are positive towards mobility. For them however, one of the bigger issues is getting their own business process straightened out first. It is not easy to provision 1000 mobile devices to your employees, and expect them to work with them just like that."

[EXP04] "It appears that more and more links between mobile devices and ERP systems exist, because increasingly information needs to be accessible to employees on remote locations at any given time, because they are used to that based on their experience from using mobile devices privately. Because more and more information is accessed through mobile devices, potentially of sensitive nature, organizations increasingly want control over them. Especially iPads and other tablets are being used for mobility, most of which still considers simple or internal tasks. The last 4-5 years security has gotten more attention on the corporate agenda, mostly because of the public exposure organizations fear to face. However, organizations still often decide to pay less attention to security when confronted with associated costs and time requirements."

[EXP05] "ERP mobility will keep growing the next coming years. The separation between older employees and younger ones with regards to adoption of mobile devices is one that will fade. Mobility will keep shifting towards one multi-purpose central device. The distinction between pocket-sized devices and larger tablet devices will remain however. Some processed are simply performed better on relatively larger devices while other fit perfectly on a smartphone, depending on the complexity of the device. This is mainly a usability issue."

ERP mobility usage

Interviewees were asked about their thoughts on ERP mobility usage, and where they thought its true value lies. Moreover they were asked for what purposes and processes mobility is being used most often now, and how they think this should change or not.

Most interviewees agreed that mobility as an extension to existing ERP systems in its current state mainly involves data entry on the one hand, and reporting functionalities on the other. Moreover, all interviewees mentioned that mobility needs to deliver something extra, i.e. it needs to be of added value somehow compared to the traditional way of executing a certain business process in order for it to become widely adopted.

[EXP01] "At some organizations it is simply the case that management does not want their employees being able to access the ERP system from certain remote locations, for instance an employee on holiday on a camping site in France. Moreover there are typically two extremes when it comes to adopting mobility in ERP environments. Organizations either do not adopt it at all because they feel like it is not secure enough, or they adopt it without really thinking it through and see where it goes from there."

[SUP01] "An important question considers which functionalities will be covered by mobile, which processes should be supported, and how mobility should be designed based on that. Should one app be developed to cover a wider variety of functionalities, or an app separately for each module or process? For now, it is better to opt for one integrated app, because it is easier to decompose an app later on than vice versa. Signals such as to-do tasks, inbox, and other workflow aspects are most important with mobility, automated spontaneity as we call it."

[EXP02] "Mobility usage revolves around two aspects, requests and approvals on the one hand, and reporting of information on the other. Requests can be in the form of an employee submitting a receipt, which a manager then needs to either approve or reject. Reporting can be in the form of actual reports, but also in the form of dashboards. Approvals and reporting are especially useful for the C-level management, CEO, COO, CFO, etc. In practice they do not use their laptop as much anymore as they used to but just their tablet, which is mainly used for approving all sorts of requests and for gaining insight in different reports quickly. It appears that there is a huge demand for dynamic dashboards, for instance to depict the status of important Key Performance Indicators. In the end, mobility is all about being more efficient."

[SUP02] "Mobility mostly involves processes that involve a lot of data-entry by the end-user, such as hour registration, HR processes, notifications, and approvals. It involves tasks where it is necessary to perform them on a remote location, such as a consultant who needs to register his hours when visiting a client. Approval of such data entry requests, expenses for instance, is also something supported with mobility. Another important topic involves their reporting platform, which has been made accessible on mobile devices. Reporting should however not become too heavy, since waiting a couple of minutes for a report is not desirable. There are however many conservative people also who find it difficult to transition to mobile devices, and thus do not want to. Moreover, some complex processes are simply better and more efficiently performed with traditional desktop computers, for instance when there is a lot of data to be shown or entered, or when different applications and tabs are to be used."

[SUP03] "On the reporting side there is still a lot of debate on how the format should look like on a mobile device to really obtain value from it compared to performing the same process or activity on another device."

[EXP03] "Adopting mobility relates to the difference between consuming information, and producing it. Mobile devices can very well be used to consume different types of information, but to produce large

quantities of information they are less viable compared to laptops or desktop computers. The choice for mobility is about consuming versus producing information."

[EXP05] "The impact of mobility may involve existing business processes. In some cases process will cease to exist, in others they will be altered. Take for example the hour registration process for employees. Traditionally, employees would do this once maybe twice a year, resulting in peak values on particular moments each year. Because employees are now able to access any HR related aspects any time a year, those peak values have disappeared. However, a more continuous and constant calls to the corporate service-desk now occurs. This means that the service-desk process tasked with aided employees with any HR related questions has changed".

Connectivity

Because of the connection between back-end application and mobile device, interviewees were asked what this connection should look like, and how it should be secured.

There were different perceptions of how mobile device can best connect to the back-end application. Some preferred native apps over responsive websites, others vice versa. All interviewees however did agree that ensuring this connection between mobile device and application is secure is of high importance.

[SUP01] "It is not set in stone to have a native app as an extension to your back-end system. The value of using a native app instead of a responsive website is partly about user experience, but on a functional level there needs to be more added value than just that. There has to be something you can and want to do on a mobile device with a native app, something you cannot, not as well at least, on a desktop computer or through responsive websites."

[SUP02] "With regard to different connectivity types, this seems to be dependent on the process being supported. Generally speaking, native apps should be used for input processes, such as expenses. Native apps are more suitable for this because this way users can benefit from device-specific functionalities, such as the camera or microphone. Offline availability is very relevant and useful for input-processes such as expenses. If an employee is traveling for instance and needs to submit an expense report, information can be entered on the go, specifying the costs and involved colleagues. Date, time, and location are automatically added. When a secure connection is re-established the data will synchronize and actually submission of data is performed. For reporting purposes this is less useful, because reporting requires data to be retrieved from the system live. Responsive websites are better suited for reporting purposes."

[SUP03] "The connection between the app on the mobile device and back-end application is always a secure connection, for instance https, and all information is retrieved through this connection. No data is stored on the device itself."

Risks

After having discussed the general concept and evolution of ERP mobility, associated relevant risks were discussed, which is what it ultimately is all about. Based on discussion from the three earlier topics, associated risks were identified.

Stunningly, it seemed that while most interviewees said organizations in general are quite aware of the impact mobile devices potentially have on their organization, current mitigation techniques were still

relatively immature, if not non-existent. This further emphasizes that ERP mobility is indeed still in its infancy and considered as a 'nice-to-have' addition, but by no means something of critical importance.

[SUP01] "From a technical perspective everything is pretty much set. Besides common technical security measures, app connectors are also used to enable the user to define what information can and cannot be retrieved by an app. From a functional perspective however, it is still very much the question what we really want to do with mobility, which means that based on the purpose of mobility risks can change. In terms of data being stored on the mobile device itself, in essence anything that is displayed on a mobile device can be considered stored on the device, either in screenshots, cache, memory, or otherwise."

[EXP02] "Many risks probably lie in the underlying process that is supported with mobility, or in existing controls in those processes, and not necessarily with mobile devices. The purchasing process for instance is an important process, because it is the only process where money is directly spent. If a fictitious supplier for instance is defined in the system and an invoice is sent and accepted, funds are directly funneled out, which means the impact of such a risk is relatively high."

[SUP02] "Data residing on the device seems not to be much of an issue. There is little to no data stored on the device itself, only the fact that a certain event took place can be retrieved. Input of data by the users which may lead to mistakes, and transmitting data to the back-end application is more important."

[SUP03] "The most worrying aspect with ERP mobility is the connection between the device and the back-end source. Many organizations still do not have any means of wiping a mobile device, for instance when employees exit the organization. Though data is not being stored on the mobile device, the user may always manually store data on the device. From an organizational perspective, such data cannot be kept within the organization. Most organizations do think of these matters, but actually managing this appears to still be in its infancy."

[EXP03] "First of all it is of course if there is an added value in using the mobile app. On top of that, to many organizations it seems adopting mobility with their ERP system is as simple as turning a switch on or off, and they have the perception that not much more is involved."

[EXP04] "The biggest risks have to do with storing data locally on a mobile device. Essentially, you do not want to store any data on the mobile device. They are easily lost, and users tend to use them not that cautiously. The more freedom you give your employees, the more risks that brings along. Allowing employees to use personally owned devices, or to install any app they want, increases the risk of losing information. Most organizations either provide a choice in mobile devices or issue one particular device. Moreover, the human factor remains a very big problem, one that is difficult to control. Though technically security can be ensured relatively easy, user awareness is needed to cover the human aspect. This should not be one simple course, but something that is continuously encouraged and maintained. Due to social usage of mobile devices a lot of things can happen, especially in case no PIN is required to access the device. Employees should be made aware of what they are doing with their mobile devices, and what the consequences could be, making user awareness really valuable. Also, a lot of managers are relatively speaking older, compared to lower level employees. This means they sometimes have less affiliation with mobile devices, and are thus less aware of associated risks, even though they have access to data that is most sensitive of nature."

[EXP05] “The connection between the mobile device and back-end system is very important, and needs to be properly secured. This also involves implementing proper authentication mechanisms to ensure valid information throughput. Ideally, user roles and privileges are derived one-to-one from the back-end system. Another important aspect is securing data stored locally on the device. Organizations should strive that data is not automatically accessible in case of device theft or loss. Other than that there are also a lot of risks related to project management, e.g. the risk that employees will not choose to use their mobile device for certain apps because it is not easy or user friendly enough. That would be a waste of both money and time.

Controls

As the final part of the interview, interviewees were asked about important mitigation techniques, mechanisms, and other matters, that play an important part in mitigating risks arising from mobility. Responses varied quite a lot among the group of interviewees. Some stated that implementing mobile business apps as an extension to traditional ERP system is like turning a switch on or off, while others (experts specifically focused on mobile (device) security) vouched for elaborate and extensive controls.

[SUP01] “With regard to private versus personal data on the same device, users are able to use so-called app connectors to define what data can or cannot be accessed by an app. With that however, data should only be stored in the clients’ database and not on the device itself. This decreases the impact of an event where an employee loses his or her mobile device, or when the device simply breaks down.”

[SUP02] “Besides regular mobile device management capabilities, we have a dedicated policy automation app that provides corporate mobile related policy available to the user on his or her device. This way rules and protocols related to mobility can be defined centrally, and then be distributed as requirements to mobile devices via mobile device management solutions.”

[SUP03] “Most controls are derived from the back-end application. The connection between the device and system obviously needs to be a secure one, and roles and authorizations for mobile app usage can be pulled from the back-end system also.”

[EXP04] “The only thing organizations can do is implement a solid mobile device management solution to control as much as possible, at least from a corporate point of view. The idea is to implement as much as possible controls to mitigate user-related risks, but this remains difficult. Sometimes choosing between usability versus security also remains an issue. The business then needs to decide that risk they are willing to accept. Dedicated VPN and multi-factor authentication mechanisms in combination with digital certificates together form a solid security baseline. Other measures such as geo-fencing can be used to shut down certain attack vectors, by disabling blue-tooth, NFC, GPS, and other connections when outside a defined perimeter. For smaller organizations it may be less viable to adopt a complete MDM solution. They should make their employees bluntly aware of possible consequences. PIN codes should also be five characters long instead of only four. Four character codes are cracked within 18 minutes, with five this is about ten times longer.

[EXP05] “Besides implementing technical mechanisms to secure the information processed through apps, they should be designed for a specific purpose and a specific target audience. Ask yourself: for who are we developing this app? Generally speaking a mobile app is either developed for a specific group of

employees such as field engineers, all ell employees of an organization, or in some cases customers of an organization. Dependent on the target audience apps should be developed in a certain way."

6 M-ERP Control Framework

This chapter elaborates on the construction of the M-ERP Control Framework (M-ERP CF), the main artifact of this thesis. A conceptual model including the components of the framework is already discussed in chapter 4. Combining the concept framework and insight of experts, the M-ERP CF is developed. The construction of this version of the framework starts with a transition from risk areas to control areas, followed by the M-ERP CF itself, and finally the M-ERP dashboard based on its contents.

6.1 Control areas

Taking into account the conceptual model that was mainly based on the literature study, the observation can be made that some of the identified controls are included on several occasions, to mitigate different risks. This is because different risks could be avoided or mitigated by the same (set of) control(s), resulting in multiple occurrences of the same control in the framework. This means that when this framework would be applied in practice, i.e. the controls would be tested by an IT auditor, controls that are the same (or closely related to each other) are found in different areas of the framework. Typically, this approach is not desirable. Controls may now potentially be tested multiple times, reducing the efficiency of the auditing process. Each control should be in the framework once, so that controls will not be tested several times unnecessary. To improve on this, once could simply remove all duplicate controls. This would however result in the illusion that some risks might not require any mitigating controls, since the risk attention areas remain the same, while relating controls would be removed (from that particular area).

A better solution would be to restructure the framework. Even though the actual risks arising from ERP mobility represent the essential component and reason for existence of this framework, the derived controls are what is ultimately to be tested by the IT auditor. So while the risk areas discussed in section 3.4 were excellent to capture the scope of ERP mobility related risks and fill the conceptual M-ERP Risk-Control Framework described in section 4.2, from a practical IT audit perspective overlap of controls is not desirable. Therefore, instead of structuring the framework based on Risk areas, the framework will be structured based on Control areas (areas of related controls). These areas together should mitigate the same original set of risks since controls are derived from them, and enable organizations and IT auditors to identify the areas where specific controls need to be implemented. Bluntly speaking, this is a transition from Risk areas to a new set of Control areas (Figure 20).

To facilitate this transition process from risk areas to control areas, all individual risks and controls that had been identified for the initial conceptual framework both have been put together into one group (subset A). Furthermore, the group is enriched with insights gained from expert interviews as discussed in chapter 5 (subset B), resulting in one set of risks and controls (total set). Some controls that have been added were related to risks that had already been identified, found by means of backward-traceability: deriving risks based on known controls (instead of vice versa as has happened so far). In some cases new or altered risks could be added. By connecting the individual risks to their control counterparts in this total set, the relationship between all controls and the risks they mitigate can be depicted.

If all duplicate and non-linked controls are removed from this total set, a new, smaller set of controls remains. This new set of controls is then analyzed, and relating controls are grouped together based on

their goal and context, rather than based on the risk(s) each control is mitigating (thus ending up with control areas rather than risk areas). Grouping the remainder of controls results in 5 distinct control areas:

1. **Mobile data protection program**: this area considers all mobile-related policy set by the organization to control the risks arising from mobility. This includes defining user awareness programs on common risks and best practices, End-User-License agreements, but also maintaining a centrally managed data classification and other mobile-related procedures that need to be documented.
2. **Device configuration**: this area revolves around preconfiguring mobile devices before they are distributed to employees. This includes matters such as enforcing policy on the device, security tools, and enforcement of other security settings on the device.
3. **Mobile asset management**: this area involves around one aspect of the Mobile Device Management component in the Server Tier (discussed in section 3.1.2), including keeping track of installed applications on devices, preselecting and approving apps that may be installed (through white- and blacklisting), but also separating private from corporate apps.
4. **Mobile device management**: this area involves around the other aspect of Mobile Device Management, and mainly focuses on keeping track of the mobile devices that are/will be distributed to employees, provide remote functionalities, and monitor devices for rooting or other unauthorized events.
5. **Data & Network security**: the fifth and final area is focused on securing the data stored or transmitted to and from the mobile device, as well as securing the connections through which data is transferred.

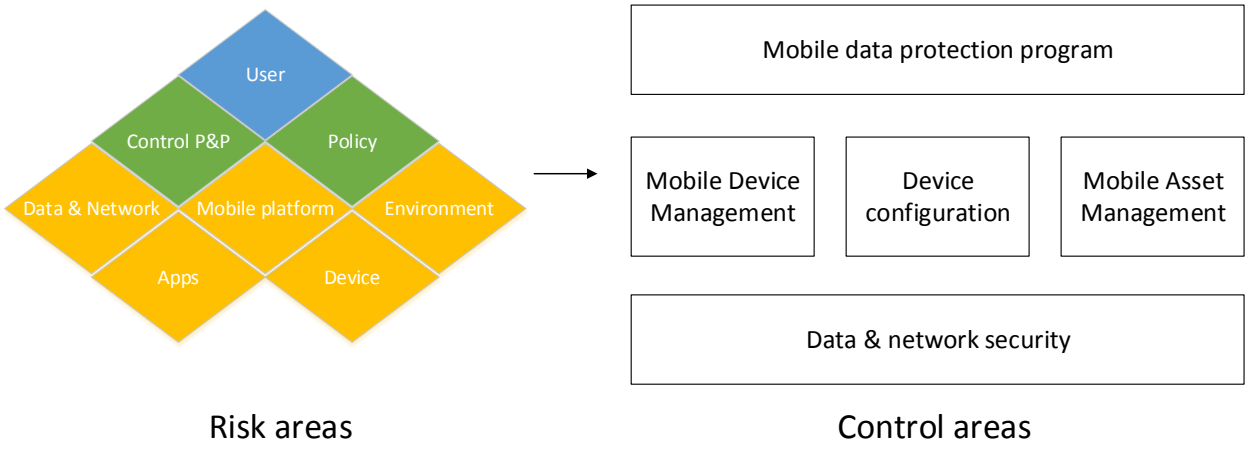


Figure 20 - Risk areas to Control areas

These 5 areas together contain a base set of controls that aim to mitigate the risks arising from mobility in M-ERP solutions. However, it remains impossible to assure that all risks have been accounted for. The framework's purpose is therefore to cover the key important risks that are relevant to organizations having adopted a M-ERP solution, to bring residual risk to a level as low as possible when applied.

6.2 M-ERP CF

Each control area (as briefly described in section 6.1) contains a number of related controls that are essential in terms of addressing relevant risks in a M-ERP solution. The five control areas with their respective controls together compose the main artifact of this thesis: the Mobile Enterprise Resource Planning Control Framework (M-ERP CF). An overview of the M-ERP CF is depicted in Figure 21. The areas are intertwined in the sense that they complement each other. It is not meant to be a choice, i.e. if an organization is in control in one area, it does not mean they are in control overall. All areas should be covered, and their respective controls tested in terms of effectiveness. Moreover it is not the case that if the framework is applied in an audit project at a certain point in time, and it appears that the organization subject to the audit is in control of its risks arising from mobility, this is then always the case from that point on. Technology will keep changing, introducing new risks, requiring changes to existing controls or additional controls, and thus again an audit on the implementation of those controls. Improving internal controls is a continuous cycle as also mentioned in section 3.3.2.

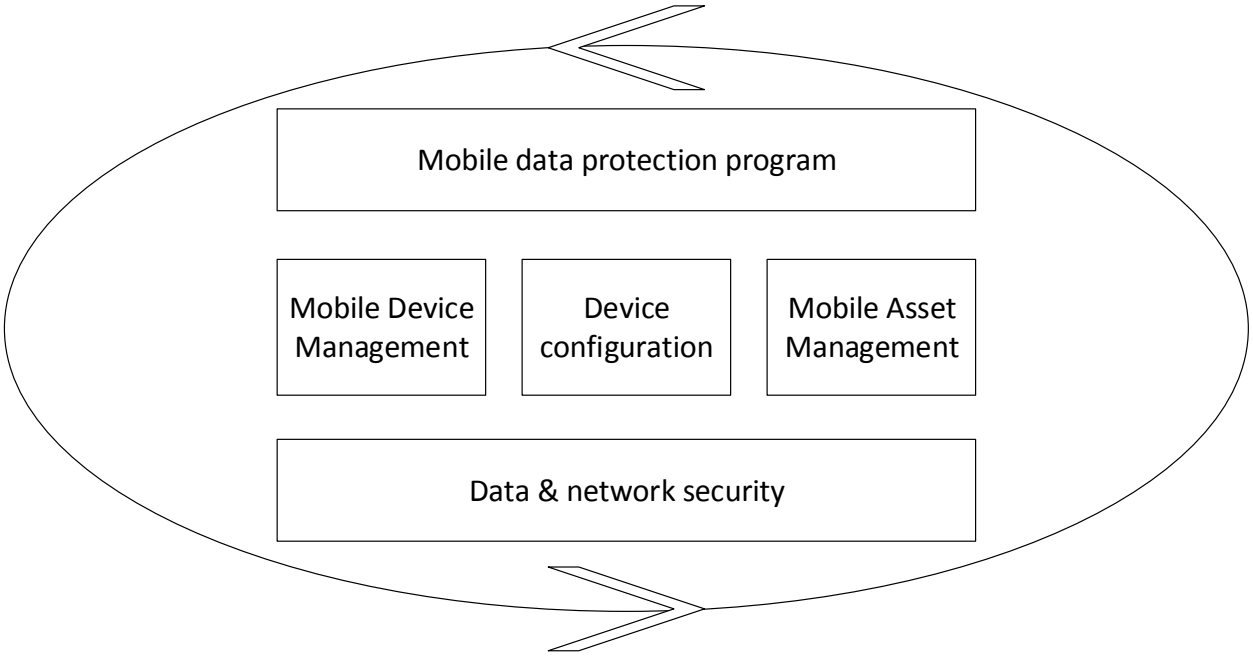


Figure 21 - Overview M-ERP CF

The importance of each control area and related controls, i.e. what risk(s) is mitigated by each control, is now discussed per area, and per control.

Mobile data protection program

The mobile data protection program control area contains three controls that together represent all policies and procedures set by the organization that relate to ERP mobility.

1.1 Data classification. A centrally managed data classification needs to be defined for data accessible through mobile devices. This avoids the risk of mixing up different types of data, mixing up data of different sensitivity levels, and users gaining access to data they should not have had access to. Moreover, this allows for easier management of data access, by linking user roles to data classes in the centrally managed data classification.

1.2 User awareness program. This control is self-explanatory, and is indeed about making users of mobile devices aware of the consequences that go with everything they do with their mobile device, and what this could mean for them personally as well as for the enterprise. The human factor remains one of the biggest problems when it comes to managing mobile devices in an enterprise as underlined by experts [E01], [E04], and [SUP01], mostly because it is simply the aspect that is least controllable. There will always be the chance that employees who lose their device, attempt to gain root access, download untrusted content, or simply do not comply to policy or regulation (either on purpose or they might not even be aware). This is why a user awareness program is necessary. It should be as simple as sending an email once a year, but it should be a program reaching employees on a continuous basis, so that employees do not forget about it and become aware of the importance of handling a mobile device in a secure and responsible manner. This could also include effectiveness campaigns, surveys, and tests to see the state of awareness among employees (e.g. a corporate-issued supposedly phishing email).

1.3 Mobile device corporate policy. This corporate policy extends the user awareness program, and should contain policies and regulations about every aspect related to mobile devices in the enterprise, and using them as a gateway to the back-end application. On the one hand such as policy is of great importance to avoid the situation where employees do not know what to do in case of lost or stolen devices, damaged ones, but also with software updates. On the other hand such a policy is important from an enterprise perspective, to ensure there is no ambiguity when it comes to who is responsible for loss of data, and to ensure employees know exactly what the organization is or is not allowed to do with data on the device. This is particularly the case in BYOD environments, since the distinction between personal and corporate data may be hard to identify (more so compared to CYOD environments, or organizations where corporate devices are simply issued to their employees).

Device configuration

The device configuration control area consists of four controls. All controls relate to technical configuration of the device before it is commissioned to an employee (pre-configuration), and involves controls that specify how devices should ideally be configured.

2.1 Policy configuration. The mobile device corporate policy that has been defined (control 3) contains elements that are configurable on the mobile device. This does not involve procedures that should be followed by employees in certain situations, but configuration requirements such as the fact that users are required to complete a certain form of user authentication before gaining access to the device. This can be configured into the mobile device, so that a user will not be able to change this configuration, i.e. removing the user authentication functionality from the device.

2.2 Security tools. Like conventional PC's being susceptible to viruses and other types of malicious software and thus in need of anti-virus software, mobile devices are subject to similar risks and thus need similar forms of protection. Besides configuring the device according to corporate policy mainly to manage risks that have to do with the user of the device, security tools (e.g. antivirus software) should therefore also be installed to protect the device from being attacked by attacks of technical nature.

2.3 Secure containers. Each business app has its own specific purpose, and data processed through these apps should typically not be mixed or intertwined with data processed in personal apps on a device. From a business perspective, data in different apps should be kept separate from one another to ensure its

integrity. Moreover, should a specific app be subject to a malicious attacker allowing the attacker access to data processed through this app, it is typically goal to limit his access as much as possible. The amount of data the attacker overall will have access to (also from apps other that the one originally attacked) will want to be minimized. This is achieved by implementing secure containers or sandboxed environments, so that an actor with access to one app does not immediately has access to another.

2.4 User authentication. User authentication ensures input issued from a mobile device is trustworthy. User authentication should first and foremost be implemented for initial device access, so that people other than the device owner will not have access to any functionalities on the device. Should other individuals gain knowledge of your user authentication mechanisms however (most often a PIN code or visual pattern), that person would have access to anything on or accessed through the device (based on the Single-Sign-On principle). PIN codes or visual pattern can either be retrieved by means of shoulder surfing (which is fairly easy with 4-character PIN codes or non-repeatable visual patterns), or even by means of "smudging" (i.e. recognizing a PIN code or pattern based on smudges on a device's screen). It is therefore desirable to have separate more extensive authentication mechanisms for apps that access more sensitive information.

Mobile Asset Management

Mobile asset management (also referred to as MAM) is about ensuring all assets on the mobile device (data & apps) are secure and managed properly. The area contains five controls that mostly relate to managing apps and maintaining their integrity.

3.1 Selective management. Ensuring a separation of business and private apps and data is especially important when considered in BYOD environments, where employees are allowed to use any personally owned mobile device within the corporate environment. In BYOD an organization typically has less control when it comes to managing a mobile device through MDM capabilities. This means that the user has more freedom, and is able to essentially install any software onto the device, potentially of malicious nature. To minimize the impact of such an event taking place, selective management is implemented, so that corporate data is not accessible, not even when a device is compromised.

3.2 White- and blacklists. As appeared from literature findings discussed in chapter 3, many apps in the Google play store (and iOS app store to a lesser extent) contain malicious software. By defining a whitelist for apps that have been analyzed and approved for installation, and a blacklist for those that have not, the risk of installing malicious apps is significantly decreased.

3.3 App development. While all other controls mitigate risks related to mobile device usage, they are all dependent on the fact that the app itself is designed in a secure manner. If an app is written poorly, a device may be configured perfectly according to corporate policy, but an attacker might be able to access data through misuse of the app, for instance by means of reverse engineering the code and adding some hidden functionality. It is therefore imperative to follow a set of guidelines that help minimize the chance of such events taking place.

3.4 App expiration duration. If after a particular duration no actions have been initiated by the user, it is typically the case that he or she is done using it for the time being. Therefore, it is unnecessary to maintain access to the app. As with having separate user authentication mechanisms for device access and specific apps, implementing a defined app expiration duration (defining how long it takes for a user to

automatically be logged out from an app) helps minimizing the chance of non-authorized individuals accessing business apps (and data). If access to an app is maintained indefinitely, an individual who gains access to the device will always be able to use that particular app and thus access the data processed through it.

3.5 App monitoring. Apps that have been included in the corporate whitelist of apps, and have been installed on a mobile device, will change over time. Either in terms of adding functionality, but more importantly also in terms of security updates. In case such updates are available, they should be analyzed in terms of what they will change, and if approved be pushed to all users having installed the app on their device.

Mobile Device Management

The Mobile Device Management (MDM) control area involves aspects that ensure mobile devices themselves are secure and managed properly. The area contains 4 distinct controls that relate to managing mobile device in an organization.

4.1 Remote functionalities. As has become apparent throughout this thesis, the mobile device and user of such a device more specifically are the most uncontrollable elements in the M-ERP environment. For this reason several capabilities are required in case such events take place, as they probably will. Employees will lose their mobile device, break it by dropping them on the ground, or they will be careless which will result in theft of mobile devices. In other words, they will lose access to their device while other unauthorized people will gain it. It should therefore be possible to lock, kill, and wipe mobile devices in case unauthorized parties gain possession of it.

4.2 Lockout recovery. If devices are locked for any reason (e.g. an employee cannot find his/her device) the device should locked in accordance with control 4.1. Should the lockout however no longer be required (e.g. an employee has found his/her device again), the data on the device should become accessible again. It should not be the case that data is indefinitely no longer accessible anymore after a device lock (data could also be backed up in a corporate cloud service).

4.3 Monitoring. It is always the case that certain risk will remain to exist (so-called residual risk) i.e. it is impossible to mitigate all the risks posing an organization. To keep track of everything related to mobile device usage, different events and aspects should be monitored. This is a typical reactive control to ensure incidents are detected once they have occurred, incase other controls may have turned out to be ineffective.

4.4 Geo-fencing. In certain situations, it may be desirable that an app is only usable in a particular physical environment. By setting geographical boundaries using GPS data from the mobile device, an organization can enforce control on where a particular app is being used. It could for instance be the case that employees are only allowed to use a particular app inside the corporate building.

Data & network security

The fifth and final control area involves securing the data on mobile devices, and the network over which it is transmitted. The area contains four distinct controls, each with a number of sub-controls.

5.1 External cloud services. The thing with external cloud services is that they cannot be controlled by an organization, and typically their security measures are inferior to those available. It is therefore best to deny employees access to such services from their mobile device (and other laptops for that matter). It

should be noted however that an enterprise-issued cloud service should ideally be provided to employees. If not, employees will most likely look to bypass controls, and find ways to access external cloud services without the organization being aware of it.

5.2 Secure connection. As stipulated by several of the experts that have been interviewed (SUP02, SUP03, E05) the connection between the mobile device and back-end application is of utmost importance. Third parties may try to intercept or drop in to the connection to steal or modify data transferred over the connection. The connection should therefore be kept secure by means of different mechanisms such as encryption and usage of digital certificates, so that the chance of meddling with this connection by unauthorized is minimized.

5.3 Data in transit. This control is closely related to control 5.2, and involves the data being transferred over the connection. Apart from securing the connection, the data in transit should be secured also, in case sub-controls included in control 5.2 appear to be ineffective or bypassed. The data in transit should therefore be separately secured, and an organization should not perceive this to be unnecessary and simply rely on other related controls.

5.4 Data access and storage. Stored data (data at rest) may be subject to attacks from hackers, lost due to incautious behavior of employees, and accessed by unauthorized individuals. Apart from controls related to data in transit separate controls should thus be in place for data storage, as well as access to this data. This involves general guidelines for users on what data not to store on their device on the one hand, and specific controls designed to ensure data is not being stored longer as required nor being accessed by the wrong persons.

6.2.1 Control framework

As a result of the transition process, the control framework could be constructed. The interplay between controls in the different areas is important, as they complement each other. The complete M-ERP CF includes specific controls specifying what should be implemented in the organization undergoing the audit, i.e. the organization at which the framework would be applied. The complete M-ERP CF is presented in Table 11.

Control area	Control	Description
Mobile data protection program	Data classification	A documented centrally managed data classification is defined, stating what data may be accessed by whom through mobile devices. A classification of data can be made based on the value of each set of data, for instance in terms of the type and sensitivity of data. Data should be processed, stored, and used according to this classification.
	User awareness program	Define a user awareness program including data management risk, network connectivity risks, common cyber threats, tips, and best practices.
	Mobile device corporate policy	* Lost/stolen procedure - Define a procedure for employees in case of a lost or stolen device. * User authentication - Define policy that states user authentication is always required, and additional user authentication is required for high-profile business apps.

Control area	Control	Description
		* Define policy on when and which remote functionalities are to be used through MDM capabilities * Define a privacy policy that covers the usage of personal information being stored and transferred on and through the device.
Device configuration	Policy configuration	Preconfigure mobile devices according to policy. Bypassing mobile device configurations should be monitored as described in control 4.3.
	Security tools	Pre-install mobile device security tools that scan apps for vulnerabilities, including antivirus software.
	Secure containers	Implement secure containers/sandboxing to ensure separation of apps and their data.
	User authentication	Require user authentication before granting access to the device: * Allow PIN numbers of more than 4 characters if possible with the mobile OS * Allow repeated patterns for swipe-based visual passwords * Ensure passwords and keys are not visible in cache or logs * Do not use a generic shared secret for integration with the back-end * Use multi-factor authentication for high-profile apps
Mobile asset management	Selective management	Implement selective management to separate business and personal apps and data on the device in case employees are allowed to use their personally owned mobile devices.
	White- and blacklists	Define and enforce white- and blacklisting of apps, to have clear insight in apps that should not be trusted. Screen apps before adding them to the whitelist, and track apps for security updates.
	App development	Define app development guidelines if a development platform is used: * Apply the principle of minimal disclosure by only collecting and disclosing data that is actually required by the app * Possibly include application-specific data-wipe capabilities with strong user-authentication * Only distribute apps via official app stores and provide feedback mechanisms that employees can use in case of security problems * Apply some sort of user input validation to ensure input is valid. Whitelist, Blacklists, or filtering may be used, often referred to as input sanitization.
	App expiration duration	Implement a mechanism so that the user is logged out of business apps after a defined amount of inactivity.

Control area	Control	Description
	App monitoring	Monitor apps on devices in terms of updates that should be installed, and push updates to all devices when needed.
Mobile device management	Remote functionalities	Use remote device wipe/reset/kill/lock functionalities according to corporate policy.
	Lockout recovery	Ensure data can be recovered from a locked device should this be necessary.
	Monitoring	Ensure the following is being monitored: * Audit log - Maintain an audit log of events and activities. * OS version control - Monitor mobile devices in terms of operating system versions, and push updates when available and validated. * Root detection - Implement a solution that detects a mobile device becoming rooted. Should such an event occur, appropriate action as defined in corporate policy should be initiated. * Ensure the back-end keeps track of events triggered by mobile devices, and retains a log of this.
	Geo-fencing	Restrict access to data or apps based on the mobile device's location, for instance allowing certain high profile apps to be only used inside the office.
Data & network security	External cloud services	Restrict access to external cloud services such as Google Drive, Dropbox, and OneDrive.
	Secure connection	Ensure the following: * Use strong and well-known encryption techniques such as AES * Enforce end-to-end secure channels such as SSL/TLS * Use certificates signed by trusted certificate authorities * Only allow establishment of a connection after verifying the identity of the remote end-point by ensuring they have a trusted certificate To further secure the connection between mobile devices and back-end system implement: * session tokens * one-time passwords * multi-factor authentication * dedicated VPN connection
	Data in transit	Ensure the following for data in transit: * Encrypt data that is being transmitted over the connection between the mobile device and the back-end application * Do not use SMS, MMS, or notifications to send sensitive information

Control area	Control	Description
		Also periodically check if sensitive data is unintentionally transferred to mobile devices, such as location information being included as meta-data.
	Data access and storage	Ensure the following: * Store sensitive data on the server and not the mobile device * Encrypt files that are locally stored on the mobile device * Develop apps so that they do not store data beyond the period required by the app. * Assume shared storage is untrusted and include this in user awareness programs * Define maximum retention periods based on which sensitive personal data gets deleted * Define and enforce control on who can access and store data through/on mobile devices, in consensus with the mobile data classification defined in the mobile data protection program

Table 11 - Control areas and controls

6.3 M-ERP CD

A dashboard is developed based on the framework presented in Table 11, as described in section 1.7.2. In essence, the tool supports the auditor throughout the entire audit process, from its inception to end. As described in section 3.3.2 the IT audit process can be seen as a check as part of the broader risk internal controls improvement cycle.

As stated, the IT auditor starts with determining what risks are applicable, and thus what controls will need to be tested by the auditor. The tool supports the auditor in the scoping process by linking risks to controls. Based on the project scope (i.e. applicable risks in a specific organizational context) the tool will provide a set of applicable controls that should be implemented, and should thus be tested in terms of their effectiveness. Once the right set of controls is identified, the tool provides support in documenting testing procedures as well as presenting results.

Based on input from the auditor during the audit, the tool provides insight into the state of effectiveness of the controls that have been tested in each of the control areas. Results of the overall assessment are then depicted in a high level overview of all areas, and the user may zoom in on each area for more detailed information, including an overview of ineffective controls for each area. Bar-charts are used to depict the state of controls in the overall assessment for easy comparison between the areas, whereas pie-charts are used for area-specific information.

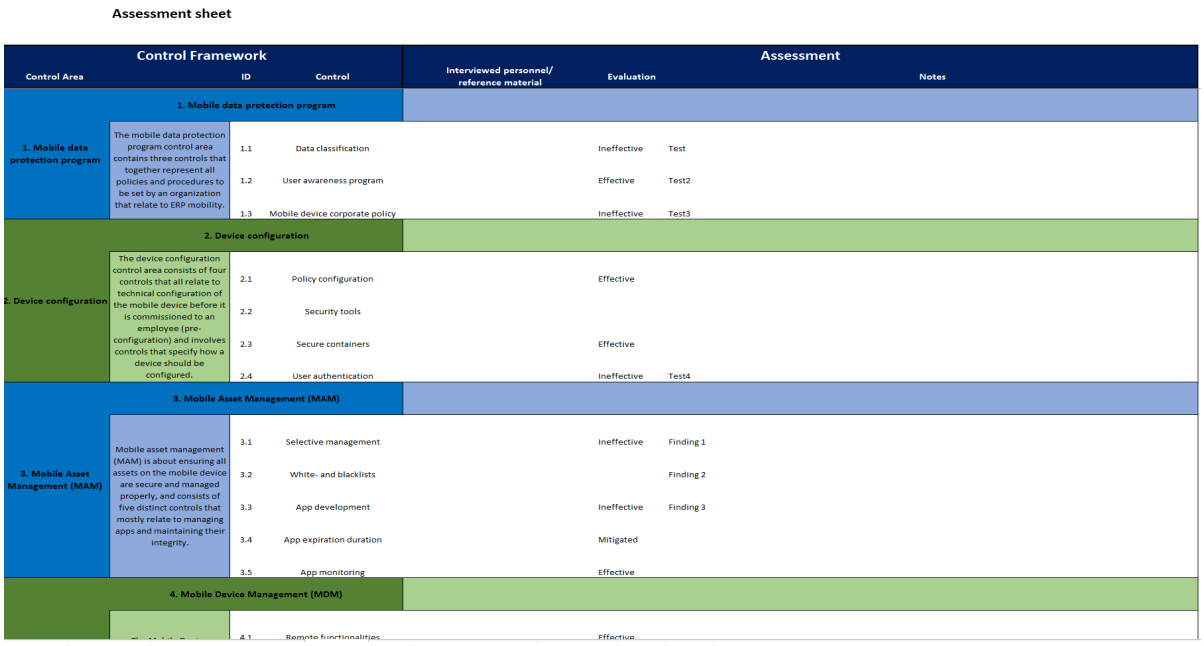
The dashboard is composed of five elements:

1. Risk assessment: An overview of the identified key risks that arise from ERP mobility. Each risk is marked with an ID-number, given a name, and a brief description;
2. M-ERP control framework: A static overview of the control framework as described in section 6.2. Risks are linked to controls in the overview using risk ID-numbers. Based on discussing risks

with their related controls a project scope can be defined for the audit, resulting in a set of controls that should be tested in the audit;

3. Assessment sheet: An assessment sheet that can be used to document tested controls, including interviewed personnel or reference material, an evaluation of the test, and additional notes;
4. Results overview: An overview of results for the entire audit, including total, effective, ineffective, and not yet tested controls;
5. Results per area: A more detailed presentation of results per control area, including total per area, effective, ineffective, not yet tested controls. A summary of ineffective controls is added, including notes that have been documented in the assessment. Furthermore a final risk evaluation of findings is depicted in a risk matrix, based on the impact and likelihood estimates of risks related to the ineffective controls.

From an audit perspective the automatic link between performing the audit (assessing control effectiveness) and the results of the audit (findings of ineffective controls and related risks) is most valuable. The assessment sheet provides support in testing relevant controls for the audit at hand, depending on the risks deemed applicable during the scoping phase. Each control that should be tested may be marked with a status (either 'Effective', 'Ineffective', 'Mitigated', or 'Not tested'), and includes input fields for evidence or other sort of input used to test the control. Note that the 'Not tested' status cannot be explicitly opted for. The results will simply show as 'Not tested' if no value has been specified. The input fields for evidence could include reference material such as documented procedures or policies, information obtained through inspecting the system itself, or information gained through interviewing relevant personnel in the organization subject to the audit. The 'Not tested' status is added to depict a control has not been tested yet, for any reason, but still should be. This is especially helpful when controls could not be tested at a certain moment for instance due to unavailability of evidence, but still needs to be tested later on. A part of the assessment sheet is depicted in Figure 22 (also added as Appendix G.3 for a larger view).



Assessment sheet

Control Framework				Assessment		
Control Area		ID	Control	Interviewed personnel/ reference material	Evaluation	Notes
1. Mobile data protection program			1. Mobile data protection program			
1. Mobile data protection program	The mobile data protection program control area contains three controls that together represent all policies and procedures to be set by an organization that relate to ERP mobility.	1.1	Data classification		Ineffective	Test
		1.2	User awareness program		Effective	Test2
		1.3	Mobile device corporate policy		Ineffective	Test3
2. Device configuration			2. Device configuration			
2. Device configuration	The device configuration control area consists of four controls that all relate to technical configuration of the mobile device before it is commissioned to an employee (pre-configuration) and involves controls that specify how a device should be configured.	2.1	Policy configuration		Effective	
		2.2	Security tools			
		2.3	Secure containers		Effective	
		2.4	User authentication		Ineffective	Test4
3. Mobile Asset Management (MAM)			3. Mobile Asset Management (MAM)			
3. Mobile Asset Management (MAM)	Mobile asset management (MAM) is about ensuring all assets on the mobile device are secure and managed properly, and consists of five distinct controls that mostly relate to managing apps and maintaining their integrity.	3.1	Selective management		Ineffective	Finding 1
		3.2	White- and blacklists			Finding 2
		3.3	App development		Ineffective	Finding 3
		3.4	App expiration duration		Mitigated	
		3.5	App monitoring		Effective	
4. Mobile Device Management (MDM)			4. Mobile Device Management (MDM)			
		4.1	Remote functionalities		Effective	

Figure 22 - Screenshot dashboard 'Assessment sheet' view

To the management of the organization subject to the audit, the results of the audit are most interesting. A screenshot of the 'Results' view of the M-ERP dashboard is presented in Figure 23. It is roughly divided into 3 areas. The top area of the overall assessment view (Figure 23 – Red rectangle) presents all five control areas, both in a spider and bar charts. The spider chart provides a quick overview of the audit result. Should the spider chart be without red, this would mean none of the tested controls was found to be ineffective. The bar charts each represent one of the five control areas. For each area it depicts the number of controls that were tested effective (green), ineffective (red), mitigated by another control (orange), or not tested yet (white).

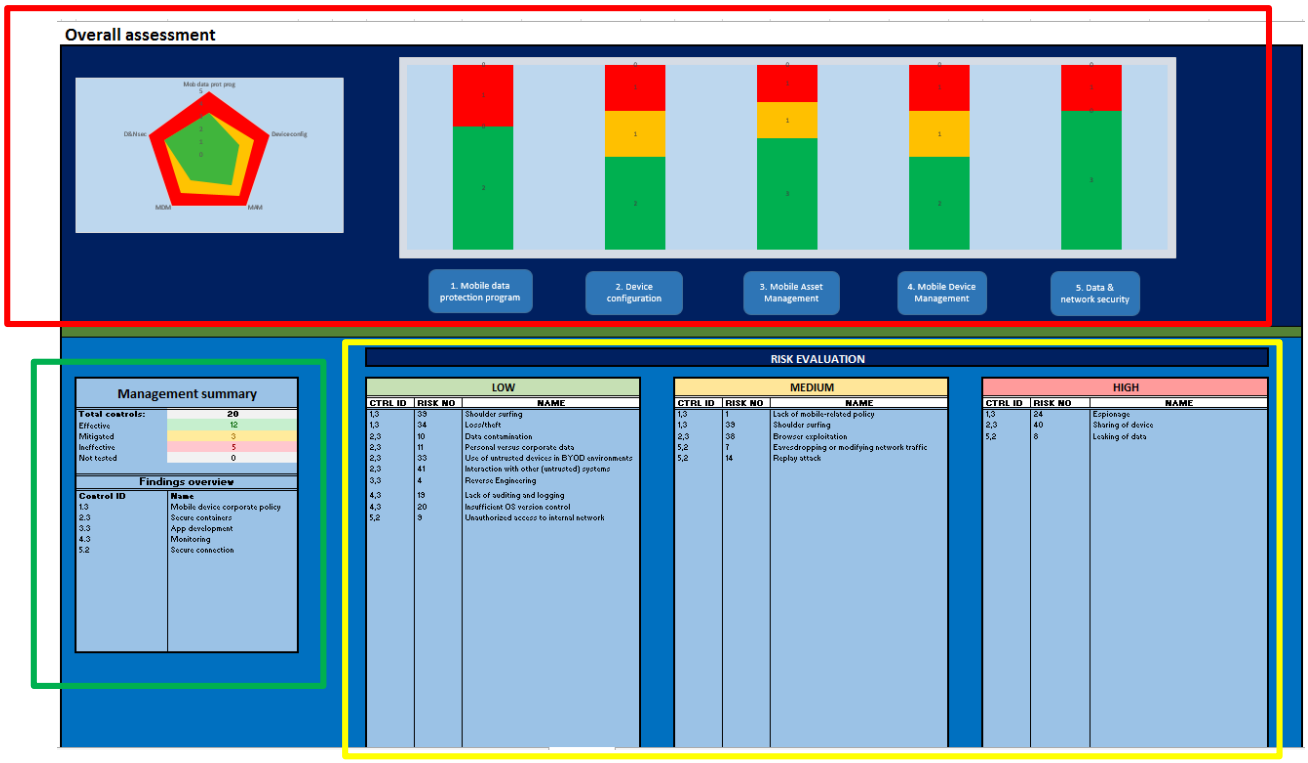


Figure 23 - Screenshot dashboard 'Results' view

The lower left corner of the overall assessment view (Figure 23 – Green rectangle) shows a summary of the audit. It present the total number of controls as well as how these were tested, and furthermore lists all ineffective controls. This provides the reader with the basic results of the audit, i.e. controls tested to be ineffective (commonly referred to as 'Findings').

Finally the lower right area of the overall assessment view (Figure 23 – Yellow rectangle) provides a brief evaluation of all the risks related to the control that have been tested to be ineffective (listed in the management summary). The risk evaluation part of the overall assessment is in itself divided over three areas: 'Low', 'Medium', and 'High' risks (Figure 24 – Screenshot dashboard 'Risk evaluation' view). The table to the left shows risks that are relatively of low importance, the middle table shows risks of medium importance, whereas the table to the right shows risks that are of critical importance, in the sense that the combined result of their impact and likelihood is high.

RISK EVALUATION

LOW

CTRL ID	RISK NO	NAME
1,3	39	Shoulder surfing
1,3	34	Loss/theft
2,3	10	Data contamination
2,3	11	Personal versus corporate data
2,3	33	Use of untrusted devices in BYOD environments
2,3	41	Interaction with other (untrusted) systems
3,3	4	Reverse Engineering
4,3	19	Lack of auditing and logging
4,3	20	Insufficient OS version control
5,2	9	Unauthorized access to internal network

MEDIUM

CTRL ID	RISK NO	NAME
1,3	1	Lack of mobile-related policy
1,3	39	Shoulder surfing
2,3	38	Browser exploitation
5,2	7	Eavesdropping or modifying network traffic
5,2	14	Replay attack

HIGH

CTRL ID	RISK NO	NAME
1,3	24	Espionage
2,3	40	Sharing of device
5,2	8	Leaking of data

Figure 24 - Screenshot dashboard 'Risk evaluation' view

The way in which risks are categorized is calculated based on their impact and likelihood values. Each risk has been given an ID number in the risk assessment view. In the data sheet that processes and links all the data between the different views together, each risks is given two parameters, one for impact and one for likelihood. Both have a value ranging from one to three. The eventual 'importance' of each risk is then calculated by multiplying the impact value with the likelihood value. As a result, each risk has an importance value ranging from one to nine (Figure 25).

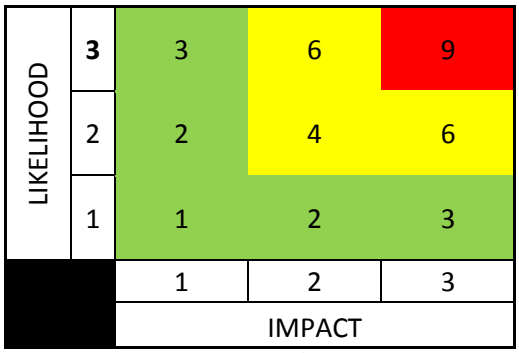


Figure 25 - Risk quantification matrix

Based on the value presented in figure 25, risks can thus obtain a value of 1-4, 6, or 9. The 'Low' importance risk group contains the green risks, with values ranging from one to three. The 'Medium' importance risk group contains the yellow risks, with values four and six. The 'High' importance group contains risks with the highest importance value nine. This means that both impact and likelihood values of the risk were value at three.

While the overall assessment provides most important information, more details on specific ineffective controls may be desirable. For this reason each control area has its own view, access from the 'Overall assessment' view. Figure 26 depicts the area view for control area 3 'Mobile Asset Management (MAM)'.

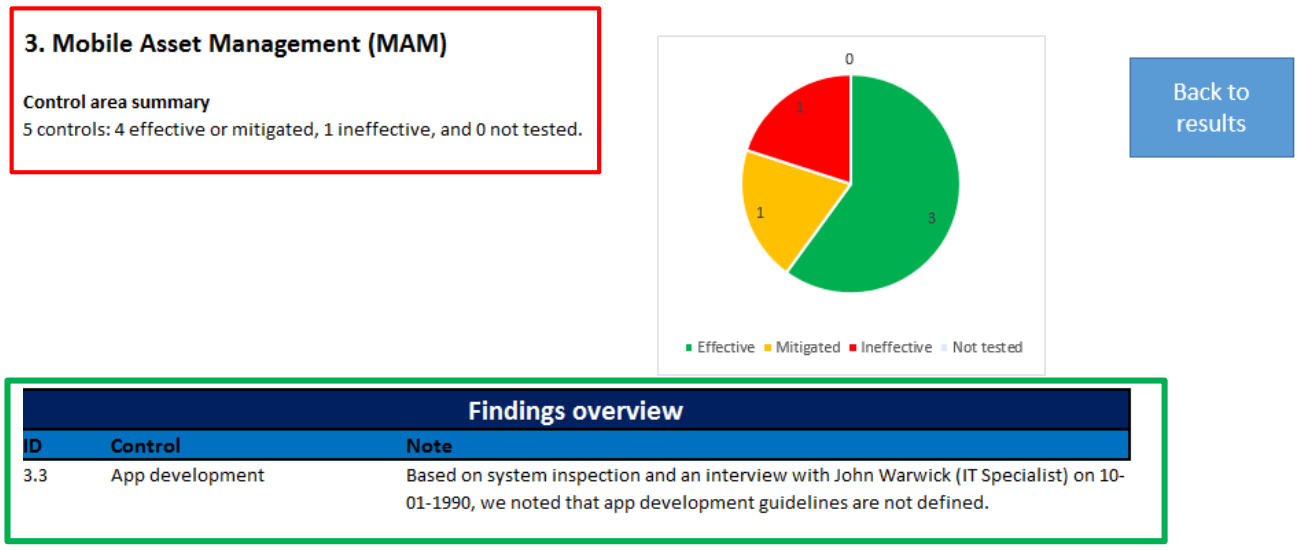


Figure 26 - Screenshot dashboard 'Control area' view

The control area view is again composed of a number of sections. The top left corner (Figure 26 – Red rectangle) presents a summary of the controls that are specific to this area. Besides showing the evaluation result of testing controls (e.g. effective), it also shows the auditor the status of testing activities, by summarizing the amount of controls that still need testing.

Furthermore, the lower section of the control area view elaborates on the controls that were listed in the overall assessment management summary, by means of a 'Findings overview' (Figure 26 – Green rectangle). Since the overall assessment views depicts in which control areas findings are noted, the dashboard is able to zoom into each area and provide further details on these findings. Such further details include the notes that were added by the auditor during testing activities, in the assessment sheet of the dashboard. This generally involves the following information:

- Explanation of why the control is concluded to be ineffective
- What information is used to come to that conclusion
- Whom at the organization subject to the audit was interviewed
- Why this person was applicable for this (function)
- The date of performed testing activities

Screenshots of all the views in the dashboard have been added separately as appendices G1 – G5.

7 Validation

7.1 Case study

To validate the research and main artifact of this thesis, the control framework is applied in a real-case environment. In other words, the control-framework is applied at an organization in which a M-ERP solution is currently being used, to evaluate their state of control in terms of mitigating risks that arise from ERP mobility. In essence this means that a process was initiated where the case company would be subject to an audit as if an actual IT auditor would audit their ERP mobility solution. This process roughly includes four steps:

Step 1 – **Scoping**: The first step in the case study is scoping the project, i.e. determining to what extent different risks are relevant for the organization at hand. As a result of the scoping process, the auditor and responsible organization at the case study organization reach a consensus on which controls need to be implemented effectively at the organization. This set of controls is considered the scope of the project, and represents the minimum set of controls the organization MUST have implemented, and can thus be considered as a base value.

Step 2 – **Gathering evidence**: After the scope of the project has been determined, the auditor and auditee know which controls need to be implemented and thus which controls need to be tested in terms of their effectiveness. To test controls, evidence needs to be gathered by the IT auditor in conjunction with the client (the case study organization). Evidence is required to verify and prove controls function effectively, and it may be gathered with different employees within the case study organization. If for instance particular parts of the system need to be viewed for which only a few employees have access to, the auditor will need to do so with one of those employees.

Step 3 – **Reporting**: After all available evidence has been gathered for the controls specified in the project scope, the auditor must report their evaluation for each of those controls. Usually this includes when the test was performed, what evidence is used to support the evaluation, with whom evidence was gathered and what role this person has, and what the results of the test was. Should evidence show the control is effective, it may be marked as 'Complete' or 'Effective'. Should evidence show the control is ineffective, i.e. show that that what is stated in the control is explicitly not the case, it should be marked as 'Ineffective' or 'Finding'. In case no evidence could be provided to test the control, for instance because evidence could simply not be found, access to evidence is restricted, or because there is no evidence, the control will have to be marked as 'Incomplete' or 'Finding'. The auditor must then specify that the control could not be properly tested due to a lack of evidence, and moreover why this is the case.

Step 4 – **Discussion**: Once all testing procedures of controls have been conducted and documented, the results of the audit (its 'Findings' most notably) will be discussed with the client. This discussion mainly involves discussing those controls that appeared to be ineffective, and what risks this poses to the organization. Depending on the type of audit the project may end with handing over the audit results to the client, at which point the client can decide what they want to do with the results (i.e. whether they want to improve their ineffective controls or not). This then thus concludes the audit, and marks the end of the project. In some cases the audit must be performed by an accredited third party, and assurance needs to be given over a set of controls. This is not taken into account within this thesis.

Step 5 – **Case study evaluation**: As a final step in the case study process not only the results of the audit are discussed from the client's perspective, but also from an auditor's perspective. This involves discussing the contents of the framework in terms of the applicability and relevance of controls, opposed to step 4 in which the results of each control are discussed. This step acts as the final iteration in the development process of the control framework, and based on the results of this step final alterations may be made to compose the final version of the control framework.

7.1.1 Case company

For selection of an appropriate company that could be used in the case study, an organization was looked for with a relevant 'mobile maturity'. Since the M-ERP CF can be seen as a general standard organizations can measure themselves against in terms of mitigating mobile ERP risks, the M-ERP CF is more applicable and usable for organizations who have a certain mobile maturity level. A small organization with only a few employees most likely has not implemented many of the controls listed in the M-EPR CF, which when subject to an audit using the M-ERP CF would result in many controls being ineffective, simply because they are not there. This would not be surprising, since for such organizations it is simply not viable nor cost-effective to implement numerous controls.

Therefore, an organization was selected with a certain level of mobile maturity. Corporate issued apps were used, mostly for HR-related tasks such as expenses, hour registration, leave, and administrative matters. Apart from taking part in the case study, an IT specialist at the case company was also interviewed prior to the case study, described in chapter 5. While the case company did not want their information included explicitly in this thesis, the following information can be provided for contextual purposes:

- Industry: Governmental
- Size: 100.000+
- Process supported with ERP mobility: Human Resources

7.1.2 Case study results

This section summarizes the results of the first four steps in the case study process as described in section 7.1. The fifth and final step (case study evaluation) is described separately in section 7.2.

Step 1 – Scoping

During the scoping process the list of risks and the five control areas of the M-ERP CF were briefly discussed in a kick-off meeting. During this meeting it already became apparent some controls in the M-ERP CF would not be present in the organization. In consensus with the case company contact person the decision was made to include all 20 controls in scope for the case study audit.

Step 2 – Gathering evidence

The approach taken in the case study was simple: the list of controls in the M-ERP CF was used as guidance in the audit. Simply put, for each control the case company contact person was asked to which extent they had implemented that particular control using the defined procedures in the M-ERP CF. For each control the case company contact person was asked how insight could be gained into the extent of which the control was implemented. For some controls this meant looking into system configuration settings (e.g. determining whether or not certain type of data or network encryption is used), while for other controls this meant looking up documented procedures (e.g. policies). In some case no information

could be provided to elaborate on the design of the control. From an audit perspective, controls where no supportive documentation or other type of information (evidence) could be provided, the control could not be deemed effective, as will be described in Step 3 – Reporting.

Step 3 – Reporting

All controls have been discussed with the case company contact person. Based on either observations from within the system (e.g. system configuration settings), documentation (e.g. company procedures), or information directly from the contact person himself (i.e. discussion with the case company contact person), controls have been tested to be effective or ineffective. For the sake of readability, the below table with testing results only includes columns 'Control area' and 'Control' of the M-ERP CF, extended with a column for 'Testing results'. Table 12 presents a summary of the case study results.

Control area	Control	Testing results
1. **Mobile data protection program**	1.3 Data classification	Ineffective: Based on an interview with case company contact person we understood that no centrally managed data classification is defined. Therefore this control is concluded to be ineffective.
	1.2 User awareness program	Effective: Based on an interview with case company contact person and received user awareness program documentation [Evid1] we noted a user awareness program is defined that is distributed to all employees using who have a registered mobile device.
	1.3 Mobile device corporate policy	Ineffective: Based on an interview with case company contact person we understood no policy is defined specifically related to mobile device usage
2. **Device configuration**	2.1 Policy configuration	Ineffective: no policy is defined (refer to control 1.3).
	2.2 Security tools	Mitigated: Based on system inspection we noted all apps processing corporate information are active in a secure container environment, separated from other apps on the device.
	2.3 Secure containers	Effective: Based on system inspection we noted all apps processing corporate information are active in a secure container environment, separated from other apps on the device.
	2.4 User authentication	Effective: Based on system inspection we noted all corporate apps require separate authentication (in addition to standard PIN authentication required to access the device).

Control area	Control	Testing results
3. **Mobile asset management**	3.1 Selective management	N/A: Secure containers are implemented (refer to control 2.3).
	3.2 White- and blacklists	Ineffective: Based on an interview with case company contact person we understood no white- and/or blacklisting of apps is maintained. Though corporate apps are active in secure containers (refer to control 2.3), the device itself and with that all other data on the device remains vulnerable to malicious apps.
	3.3 App development	N/A: Based on an interview with case company contact person we understood that apps are being developed by an accredited third party, specialized in app development.
	3.4 App expiration duration	Effective: Based on system inspection we noted that corporate apps are configured to automatically logout after 3 minutes of inactivity.
	3.5 App monitoring	Effective: Based on an interview with case company contact person we understood (security) updates for corporate apps are pushed too all issued mobile devices after validation.
4. **Mobile device management**	4.1 Remote functionalities	Ineffective: Based on an interview with case company contact person we understood remote functionalities may be used when needed. We noted however that no formal procedure is defined for this.
	4.2 Lockout recovery	Effective: Based on an interview with case company contact person we understood device locks may be removed by administrators in case they are no longer necessary.
	4.3 Monitoring	Ineffective: Based on an interview with case company contact person we understood the following: *Audit log: no audit log is kept of activities performed on mobile devices *OS version control: updates to the mobile OS are pushed to all devices simultaneously. OS version can however be stalled to the point where the mobile device connects to a Wi-Fi network. *Root detection: no root detection capabilities are implemented. *Back-end logging: no back-end logging capabilities are implemented.

Control area	Control	Testing results
		Based on the observations above, this control is concluded to be ineffective, because no audit log is kept, OS version updates are not enforced, no root detection is present, and no back-end logging is enabled.
	4.4 Geo-fencing	N/A: Apps are not bound to specific geographical locations, therefore this control has not been tested.
5. **Data & network security**	5.1 External cloud services	Ineffective: Based on an interview with case company contact person we understood that access to external cloud services such as Dropbox, Google Drive, or One Drive is not restricted.
	5.2 Secure connection	Mitigated: Refer to control 5.3.
	5.3 Data in transit	Effective: Based on system inspection and an interview with case company contact person we noted that data transmitted between mobile devices and back-end source are AES encrypted.
	5.4 Data access and storage	Ineffective: Based on an interview with case company contact person we understood the following: *Data is stored on the server, thin clients are used. *App development is done by an accredited third-party *Access to shared storage services is not restricted *No maximum retention periods have been defined *All registered mobile devices have access to the same set of data via corporate apps. The control is concluded to be ineffective because access to shared storage is not restricted, and no maximum retention periods have been defined.

Table 12 - Case study testing results

Step 4 – Discussion

After having reported all testing activities in Step 3 – Reporting, tests results have been discussed with the case company contact person. Since all controls have been considered in scope of the case study, each control was evaluated to be either effective, ineffective, mitigated (control itself ineffective, but another controls makes up for it), or not applicable. Non applicable controls represent a number of controls that

were deemed out of scope after discussing them more thoroughly. The overall assessment of the 20 controls in the M-EPR CF was:

- Ineffective controls: 8
- Effective controls: 7
- Mitigated controls: 2
- Not tested controls: 3

While the case company contact person agreed with most observations obtained throughout the case study, some controls that were tested ineffective were discussed in particular. Control 4.3 'Monitoring' for instance, the case company contact person replied with: "I cannot enforce employees to install a new OS version. It is simple, these updates generally consist of a lot of data which makes it expensive to updates them over the mobile broadband network. I cannot force someone to connect to a Wi-Fi network.". While a valid and understandable response, this does not take away the fact that employees may use older versions of the mobile OS even though from an organizational perspective it is assumed the updates are pushed to all devices. After having briefly discussed all observations of the overall assessment, the contents and structure of the M-ERP CF itself was evaluated.

7.2 Case study evaluation

Based on the results and discussions from the conducted case study (section 7.1) additional insight is gained on the applicability and relevance of the different controls composing the framework. A brief overview of some the evaluation comments is given below, after which a section is included describing specific modifications of the M-ERP CF based on these evaluation remarks.

7.2.1 Evaluation remarks

"Regarding control 2.4 'User authentication', and more specifically the sub-control "Do not store any passwords or secrets in application binary": while this indeed is related to user authentication is it typically ensured when developing an app. I would therefore suggest to move this sub-control from this area to the area considering app development guidelines."

"Regarding the MDM and MAM areas, I think there is significant overlap in terms of the controls they cover. Take for example the lockout recovery control. This has to do with recovering data stored on the device, and not explicitly the device overall. You would expect such a control to be included in the MAM area."

"Control 4.2 'Lockout recovery' is also an example of a remote functionality. Even though it considers granting privileges instead of restricting them opposed to the already defined remote functionalities in MDM, should this not be grouped together?"

"Control 5.4 'Data access and storage', and more specifically the sub-section about not storing data beyond the period that it is required by the app: this sub-section should not be included in this area in my opinion, even though it is related to data. This aspect should be moved to control 3.3 App development."

"With respect to the entire framework, controls should typically be defined as statements that should be present at the organization subject to the audit. As it is now, controls are defined as actions that can be executed by an organization opposed to policies, documents, or other matters that should already be there".

"Regarding control 5.2 'Secure connection', it seems to me that this control is a collection of several controls instead of just one. There is for instance encryption, a secure connection, usage of digital certificates, and several other mechanisms. You should separate these into multiple controls, since they will be tested separately in practice also."

"With respect to control 3.1 'Selective management', while the distinct boundary between personal versus corporate data may sound nice, in practice a mobile device simply is a relatively personal device, and separation between personal and corporate data can be ensured via secure containers or sandboxing implementations. The addition of implementing a selective management capability has no real added value to me."

"In control 5.2 'Secure connection', and more specifically the sub-control related to AES encryption, I feel you should move this part to the 'Data in transit' or 'Data access and storage' area, since AES is about encrypting the data itself."

7.2.2 Final M-ERP CF

Based on an evaluation of the conducted case study and its result, revisions have been made to the M-ERP CF. A summary of modifications based on the case study evaluation is presented below. The final adapted M-ERP CF can be found in appendix F.

General evaluation

A general remark on the framework related to the way in which controls were defined. The controls in the M-ERP CF presented in section 6.2.1 were written as 'activities' an organization should execute, rather than statements that can be tested. For example, control 1.2 User Awareness Program was defined as: "Define a user awareness program including data management risk, network connectivity risks, common cyber threats, tips, and best practices.". Typically when defining controls, they should be phrased in a way that one can determine whether or not that control is true or not (effective or ineffective). To do this for an activity, it is hard to determine if the activity "Define a user awareness program" is effective or not. An organization may be in the process of defining such a program. Technically that would mean they are defining a program, it is just not documented yet.

After discussing this in some evaluation interviews also, it became apparent that controls should be phrased as statements that can either be true or false, i.e. effective or ineffective. Control 1.2 could then be rephrased to "A documented user awareness program is defined, including data management risks, network connectivity risks, common cyber threats, tips, and best practices related to ERP mobility.". While this may seem like a small difference, the auditor can now explicitly state whether this control is effective or not, e.g. "yes a documented user awareness program is defined including the aforementioned aspects", or "no, no such documented user awareness program is defined". All controls throughout the M-ERP CF have therefore been revised and rephrased to statements rather than activities.

Specific controls

With respect to a number of controls, evaluation remarks were given (section 7.2.1). Based on the evaluation remarks the following adjustments have been made to the M-ERP CF:

- Control 2.4 User Authentication: one of the elements in this control related to not storing user authentication information in the application binary. This particular part of the control has been moved to control 'App development'.

- Control 3.1 Selective Management: this control overlaps with sandboxing/secure container principles. This control has been removed.
- Control 4.2 Lockout Recovery: this control was grouped in the MDM area. Since it is specifically relates to the data on the device it is moved to the MAM area.
- Control 5.2 Secure Connection: this controls essentially contains a number of sub-controls that are not related to each other. This control has been divided over 4 separate controls:
    - Secure connection: end-to-end channel
    - Secure connection: certificate usage
    - Secure connection: VPN
    - Secure connection: unique session
- Control 5.2 Secure Connection: the sub-control related to AES encryption is removed from this control and added to the control related to Data in transit
- Control 5.4 Data access and storage: the sub-control related to temporarily storing data in the app has been moved to the control related to App Development

As a result of the case study evaluation, the M-ERP CF is composed of 5 control areas, combined containing 22 controls. Below is a summary of the final M-ERP CF. The final M-ERP CF in its entirety is added as appendix F.

1. Mobile Data Protection Program
1.1: Data Classification
1.2: User Awareness Program
1.3: Mobile Device Corporate Policy

2. Device Configuration
2.1: Policy Configuration
2.2: Security Tools
2.3: Secure Containers
2.4: User Authentication

3. Mobile Asset Management
3.1: White- and Blacklists
3.2: App Development
3.3: App Expiration Duration
3.4: App Monitoring
3.5: Lockout Recovery

4. Mobile Device Management
4.1: Remote Functionalities
4.2: Monitoring
4.3 Geo-Fencing

5. Data & Network Security
5.1 External Cloud Services
5.2 Secure Connection end-to-end channel

5.3 Secure Connection certificate usage
5.4 Secure Connection VPN
5.5 Secure Connection unique session
5.6 Data in transit
5.7 Data access and storage

8 Discussion & conclusions

8.1 Conclusions

While many mobile enterprise applications already exist that may be used on mobile devices that are also integrated with back-end ERP systems, it is still an immature domain that is not far developed yet. Apps are used mostly for basic HR-related processes such as expenses and hour registration, CRM related processes, and the occasional sales task. While opportunities with ERP mobility are extensive, adoption appears to still be fragmented. Some organizations have already adopted mobile solutions whereas others do not want anything to do with it. This means that many controls that are designed to mitigate potential risks arising from mobility are often not applicable yet in organizations who use some form of mobility, simply because for them it is not viable to implement such controls. Their maturity of in terms of using M-ERP capabilities is not far developed. In other words, it may be stated that the complexity, effort, and money that go with implementing mobile-related controls, such as those proposed in the control framework presented in this thesis, do not outweigh the benefit and value they provide. It thus appears that, at least in the Netherlands, ERP mobility is still in its infancy.

SQ1: *What different types of risk exists as a result from ERP mobility, and where do they occur?*

Appendix B shows an overview of the mobile threat landscape, and Appendix E shows an overview of risks partly derived from these, categorized and mapped into 8 risk areas. A comprehensive overview of risks that were identified throughout this thesis has been discussed in chapters three and four. Most prominent areas appeared to be the 'Data & network' (13 risks), 'User' (10 risks), and 'Device' risk area (8 risks), together representing 31 out of a total of 42 identified risks. While the 'Data & network' and 'Device' risk areas are mostly technological of nature, the 'User' risk area has an obvious human nature. Furthermore it seems to be the case that the least controllable risks are found in this risk area, and mostly relate to employees who use a mobile device in their day to day business activities. It thus seems that while technologically an organization may implement a huge number of security measures, human interference potentially undermine such efforts.

SQ2: *How can each of the identified risks be mitigated and controlled?*

A comprehensive overview of controls that mitigate the earlier discussed risks represent the main elements that together compose the M-ERP CF (section 6.2) and M-ERP CD (section 6.3). With mobility, different and adjusted controls are required compared to traditional ERP environments. These controls have been grouped in five main themes: (1) Mobile data protection program, (2) Mobile Asset Management (MAM), (3) Device configuration, (4) Mobile Device Management (MDM), and (5) Data & network security. Based on the key risks that have been identified in M-ERP solutions, controls grouped into these five themes aim to help organizations become in control of their risks due to mobility.

SQ3: *To what extent can existing control frameworks related to IT risk and IT controls be used for ERP mobility?*

While existing control frameworks provide a good contextual understanding of the theoretical foundations and general application in practice, they lack mobile-specific aspects to ensure their applicability in practical environments. The essential elements that compose a general control framework are included in the M-ERP also: *Risks* that are opposed by *Control objectives,* which can be achieved by implementing

specific *Controls*, which can be grouped into a number of *Control areas*, in which each control is tested by a defined testing *Procedure* in terms of its effectiveness. Specific controls in the M-ERP CF have thus been derived mostly from other research and expert interviews, whereas the structure of the M-ERP CF is largely based on frameworks such as COBIT and COSO.

SQ4: *How do ERP mobility usage and strategies influence the risks that need to be mitigated?*

Mobile device are nowadays the main platform of engagement and changed the way of engaging information, in the sense that users no longer access ERP data just via their PC's or other conventional computers such as laptops. In essence there is a set of controls that should always be implemented in any organization where a form of ERP mobility has been adopted, regardless of the process supported by it or employee group(s) using it. Based on the processes supported with however, different information, thus data of different sensitivity levels is accessed through and potentially stored on a mobile device. Depending on the sensitivity level of such data (possibly defined in a data classification), an organization may opt to implement less or additional controls. This returns us to the weigh-off between time, effort, and money on the one hand, and security of your data on the other. The added value of mobility needs to be made clear to management in order for them to fully commit to it, and the necessity of controls that go with extended mobility usage in case they do.

From an information security perspective, what is the impact of integrating mobile technology with existing ERP environments?

The essential elements of information security have been discussed: confidentiality, integrity, and availability of information. The goal of this thesis was to identify risks that could affect any of these components with respect to information processed through M-ERP solutions. It is apparent that organizations having adopted a M-ERP solution are subject to different, altered, or amplified risks compared to traditional ERP solutions. The answer to the main research question, is depicted in the M-ERP CF. The combined set of controls in the M-ERP CF aims to capture the most important consequences that organizations are faced with when adopting a M-ERP solution. Most prevalent risks relate to changes in the data & network and mobile apps areas, while the people who actually use mobile device remain to be the least predictable and thus controllable factor. It thus appears that technological many security mechanisms can be implemented by organizations to bring residual risk to a level as low as possible, yet employees will may potentially act in ways that undermine these efforts. This is emphasized by the fact that the preliminary M-ERP Risk-Control framework (Appendix E) contains 10 distinct risks, while practically they can only be mitigated by means of educating employees, and making them aware of what may happen when mobile devices are not used with care. Furthermore, even if such educational and user awareness programs are successful, there will always be employees who lose their device or get stolen from.

All in all, the five control areas proposed in the M-ERP CF (Mobile data protection program, Mobile Device Management, Device configuration, Mobile Asset Management, and Data & Network security) provide a base set of controls that organizations should take into account when adopting some form of ERP mobility. Each area contains a number of controls that can be implemented, depending on the extent of mobile ERP usage, strategy, and perhaps even size of the organization. Some controls may be

somewhat elaborate for organization that are relatively smaller in size. For such organizations it could not be very profitable to implement certain controls. The weigh-off between controlling certain M-ERP related risks on the one hand, and not having to invest money, time, and effort into designing, implementing, and maintaining related controls on the other, may often lean towards the latter.

8.2 Discussion & limitations

ERP mobility experts from different ERP suppliers have been interviewed to compose the main artifact of this thesis. This means that one the one hand an organization who is a multi-national that operates all over the world is contacted for input, and on the other an organization with their main operations residing in the Netherlands. With regard to the case company however, this is an organization in the Netherlands and no attempt was made to contact organizations elsewhere, due to impossibilities (both practical and financial) of conducting a case study abroad, in for example the US. While the contents of the framework thus reflect ERP mobility in general, validation of the M-ERP CF was restricted to one organization, in The Netherlands. Should more organizations have been used in multiple case studies, and not only in The Netherlands but in the US for instance also, validation insights would have been gained that go beyond the restrictions due to the state of maturity in organizations adopting ERP mobility in The Netherlands.

The automatic link between output from the risk assessment and determining required controls is also one that is typically somewhat ambiguous. In practice, the risk assessment is a process typically open to subjectivity of those involved. Determining how high the impact or likelihood of particular risks are is not something that is set in stone, in the sense that depending on the type of organization, employees, and related information assets, different risks may be deemed more or less important. A limitation of the M-ERP CD is that this relation between risks and control is a static one. This means that if management of an organization subject to an audit may value risks differently, the M-ERP CD cannot take this into account. Moreover, should risks need revising, links between risks and their respective controls need to be revised also.

8.3 Future work

A great opportunity for future research is to combine the M-ERP CF with a method such as the M-RAM, to include automatic evaluation of improving controls based on risk assessments. Furthermore a methodology could be developed to take into account the difference between the initial risk of a threat occurring and the residual risk (after mitigating it with a control) of a threat occurring. This could then be a metric to determine the priority of implementing a particular control. In other words, if the difference between initial and residual risk is large, implementing the mitigating control thus has a large impact (i.e. much risks will be mitigated, because of a decrease in likelihood, impact, or both) giving it a high priority. If the difference between initial and residual risk is only small, the mitigating control has a relatively low impact, giving it a lower priority.

Other countries than The Netherlands might be more mature in terms of adopting M-ERP solutions. Two of the largest ERP suppliers on a global level are SAP and Oracle, both having their main operation of business in the US. This means that should the research described in this thesis be performed in the US instead of the Netherlands, results and thus conclusions may have been different. Performing similar case

studies in different countries should be done to get more insight in the adoption of ERP mobility on a global level, and also allows for comparisons of possible best practices in different geographical areas.

9 References

Al-Mashari, M. (2002). Enterprise resource planning (ERP) systems: a research agenda. *Industrial Management & Data Systems*. Retrieved from http://www.emeraldinsight.com/journals.htm?articleid=850073&show=abstract

Avizienis, A., Laprie, J., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing.

Bar, A. Al, & Mohamed, E. (2011). A preliminary review of implementing Enterprise Mobile Application in ERP environment. *International Journal of Engineering & Technology*, *11*(04), 60–65. Retrieved from http://www.ijens.org/Vol_11_I_04/116504-2828-IJET-IJENS.pdf

Basle Committee on Banking Supervision. (1998). Enhancing Bank Transparency, (September). Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Enhancing+Bank+Transparency#2

Bishop, M. (2000). Academia and education in information security: Four years later. Retrieved from ftp://zedz.net/pub/security/development/secure-programming/bishop-2000-academia-and-education-in-information-security-four-years-later.pdf

Bradford, M., Earp, J. B., & Grabski, S. (2014). Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the Technology Organization Environment framework. *International Journal of Accounting Information Systems*, *15*(2), 149–165. doi:10.1016/j.accinf.2014.01.003

Breaux, T., & Rao, A. (2013). Managing Risk in Mobile Applications With Formal Security Policies, (April).

Brockett, P., Golden, L., & Wolman, W. (2012). Enterprise cyber risk management. *Enterprise Cyber Risk Management*, (April). Retrieved from http://cdn.intechopen.com/pdfs/36109/InTech-Enterprise_cyber_risk_management.pdf

Cavaye, A. L. M. (1996). Case study research: a multi-faceted research approach for IS. *Info Systems J*, *6*, 227–242.

Chaganti, S; Bayne, D. (2011). Run for it!: Jailbreaking and its Effects. *Zhurnal Eksperimental'noi I Teoreticheskoi Fiziki*, 1–13. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+Title#0

Chang, S.-I., Yen, D. C., Chang, I.-C., & Jan, D. (2014). Internal control framework for a compliant ERP system. *Information & Management*, *51*(2), 187–205. doi:10.1016/j.im.2013.11.002

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731. doi:10.1016/j.cose.2011.08.004

Chuprunov, M. (2013). IT General Controls in SAP ERP. *Auditing and GRC Automation in SAP*, 131–163. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-35302-4_6

Citrix. (2013). Citrix XenMobile technology overview.

Columbus, L. (2013). 2013 ERP Market Share Update: SAP Solidifies Market Leadership. Retrieved October 22, 2014, from http://www.forbes.com/sites/louiscolumbus/2013/05/12/2013-erp-market-share-update-sap-solidifies-market-leadership/

COSO. (2011). Internal Control - Integrated Framework, (December). Retrieved from http://xml.coverpages.org/SAML20-ProfileSSO-DanishPublicSectorV11.pdf

Debreceny, R. S. (2013). Research on IT Governance, Risk, and Value: Challenges and Opportunities. *Journal of Information Systems*, *27*(1), 129–135. doi:10.2308/isys-10339

Engebrethson, R. (2012). Comparative Analysis of ERP Emerging Technologies, (May). Retrieved from http://digitalcommons.calpoly.edu/theses/739/

Ernst & Young. (2013). BYOD: Security and risk considerations for your mobile device program.

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

Fibikova, L., & Mueller, R. (2012). Threats, Risks and the Derived Information Security Strategy, *6*, 11–20. Retrieved from http://books.google.com/books?hl=en&lr=&id=VbAGHvmWPh0C&oi=fnd&pg=PA10&dq=Information+Security+Strategy&ots=XBeWS7ihUg&sig=ZCF_pvjl9x3RPJM88UL36DbvSz8

Freeman, E. (2011). Cybercrimes: A Multidisciplinary Analysis, 151–163. doi:10.1007/978-3-642-13547-7

Furtmüller, F. (2013). An Approach to Secure Mobile Enterprise Architectures. *arXiv Preprint arXiv:1304.0076*, (Mdm). Retrieved from http://arxiv.org/abs/1304.0076

Gelogo, Y., & Kim, H. (2014). Mobile Integrated Enterprise Resource Planning System Architecture. *International Journal of Control & Automation*, *7*(3), 379–388. Retrieved from http://www.sersc.org/journals/IJCA/vol7_no3/36.pdf

Gidey, E., Jilcha, K., Beshah, B., & Kitaw, D. (2014). The Plan-Do-Check-Act Cycle of Value Addition. *Industrial Engineering & Management*, *03*(01). doi:10.4172/2169-0316.1000124

Giessmann, A., Stanoevska-Slabeva, K., & de Visser, B. (2012). Mobile Enterprise Applications--Current State and Future Directions. *2012 45th Hawaii International Conference on System Sciences*, 1363–1372. doi:10.1109/HICSS.2012.435

Haddara, M., & Zach, O. (2011). ERP systems in SMEs: A literature review. *Proceedings of the 44th Hawaii International Conference on System Scieces*, 1–10. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5718924

Haex, P., Prinsenberg, M., & Niekus, M. (2014). COSO-herziening als vliegwiel voor heroriëntatie op internal control.

Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security*, *22*(1), 97–114. doi:10.1108/IMCS-03-2013-0019

Hasan, B., Gómez, J. M., & Kurzhöfer, J. (2013). Towards a Framework for Designing Secure Mobile Enterprise Applications. *MOBILITY 2013: The Third International Conference on Mobile Services, Resources, and Users*, 90–93. Retrieved from http://www.thinkmind.org/index.php?view=article&articleid=mobility_2013_4_30_40038

ISO/IEC. (2007). NEN-ISO/IEC 27002:2007, *27002*(november).

Jain, A., & Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. *IT Professional*, *14*(5), 28–33. Retrieved from http://doi.ieeecomputersociety.org/10.1109/MITP.2012.72

Janssen, J. (2013). Enterprise Mobile Security: the development of a mobile risk assessment method (M-RAM), (November).

Julie, J. C. H., & Ryan, D. S. (2011). Cyber security: The mess we're in and why it's going to get worse. *Developing Cyber Security Synergy*. Retrieved from http://www.cspri.seas.gwu.edu/uploads/2/1/3/2/21324690/2011-4_cyber_security-the_mess_were_in_ryan.pdf

Kapko, M. (2012). The Quest for Security in Mobile. *Feature Report. Juniper*. Retrieved from http://whitepapers.rcrwireless.com/junipermobilesecurity/MobileSecurity_FeatureReport.pdf

Klaus, H., Rosemann, M., & Gable, G. (2000). What is ERP? *Information Systems Frontiers*. Retrieved from http://link.springer.com/article/10.1023/A:1026543906354

Kouns, J., & Minoli, D. (2011). Information Technology Risk Management in enterprise environments. *Zhurnal Eksperimental'noi I Teoreticheskoi Fiziki*. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+Title#0

Kumar, A. (2012). Enterprise Mobility Strategy – Should Enterprises Care ?, *10*(1), 35–49.

Leavitt, N. (2011). Mobile security: finally a serious problem? *Computer*, (June), 11–14. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5875929

Lehrfeld, M. (2012). Securing Mobile Devices in the Enterprise. *Proceedings of the 2012 ASCUE Summer Conference*.

Lindow, P., & Race, J. (2002). Beyond traditional audit techniques. *Journal of Accountancy*, *194*(1), 28–33. Retrieved from http://www.caacm.com/i/u/6024308/i/last.pdf

Maan, J. (2012). Enterprise Mobility–A Future Transformation Strategy for Organizations. *Advances in Computer Science, Eng. & Appl.*, (167), 559–567. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-30111-7_53

Mansfield-Devine, S. (2013). Security review: the past year. *Computer Fraud & Security*, (1), 5–11. doi:10.1016/S1361-3723(13)70006-X

Markelj, B., & Bernik, I. (2012). Mobile devices and corporate data security. *International Journal of Education and Information Technologies*, *6*(1), 97–104. Retrieved from http://www.naun.orgwww.naun.org/multimedia/NAUN/educationinformation/17-591.pdf

McAfee, A. (2006). Mastering the three worlds of information technology. *Harvard Business Review*, (November). Retrieved from http://www.mba.handlowa.eu/docs/semestr2/IT in Management - Mastering the three wolds of information technology.pdf

Muchenje, T. (2012). An analysus of the impact of emerging technology on organisation's internal controls. *Zhurnal Eksperimental'noi I Teoreticheskoi Fiziki*, (May). Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+Title#0

National Institute of Standards and Technology. (2014). Framework for Improving Critical Infrastructure Cybersecurity, (February). Retrieved from https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=267567

NCSC. (2012a). Beveiligingsrichtlijnen voor mobiele apparaten Deel 1, (November).

NCSC. (2012b). Beveiligingsrichtlijnen voor mobiele apparaten Deel 2, (November).

Norton. (2011). 2011 NORTON CYBERCRIME REPORT.

Pederiva, A. (2003). The Cobit Maturity Model in a Vendor Evaluation Case.

Peersman, J. J. (2012). MBI Master Thesis Preventing Data Breaches by Proactive Data mining, (December).

Petticrew, M. R. H. (2006). Systematic Reviews in the Social Sciences. *Cebma.info*. Retrieved from http://www.cebma.info/wp-content/uploads/Pettigrew-Roberts-SR-in-the-Soc-Sc.pdf

Pironti, J. (2006). Key elements of a threat and vulnerability management program. *Information Systems Control Journal*, 1–5. Retrieved from http://www.interop.com/newyork/2005/presentations/downloads/paid/key-elements-of-a-threat-and-vulnerability-mgmt-program-j-pironti.pdf

Potts, M. (2012). The state of information security. *Network Security*, *2012*(7), 9–11. doi:10.1016/S1353-4858(12)70064-8

Ramamoorti, S., & Weidenmier, M. L. (2004). *THE PERVASIVE IMPACT OF INFORMATION TECHNOLOGY*.

Rhee, K., Jeon, W., & Won, D. (2012). Security requirements of a mobile device management system. *International Journal of Security and Its Applications*, *6*(2), 353–358. Retrieved from http://www.sersc.org/journals/IJSIA/vol6_no2_2012/49.pdf

Richards, K. (2009). *The Australian Business Assessment of Computer User Security: A national survey*. Retrieved from http://eprints.qut.edu.au/59178/

Rikhardsson, P., Best, P., Green, P., & Rosemann, M. (2006). Business Process Risk Management, Compliance, and Internal Control: A Research Agenda. Retrieved from http://core.kmi.open.ac.uk/download/pdf/7279056.pdf

Rodosek, G. D., & Golling, M. (2013). Cyber Security : Challenges and Application, 179–197.

Sadeghi, A. (2013). Mobile security and privacy: the quest for the mighty access control. *Proceedings of the 18th ACM Symposium on Access Control Models and Technologies*, 8–9. Retrieved from http://dl.acm.org/citation.cfm?id=2463204

SAP. (2013). SMP Security & Identity Management.

Sayana, S. A. (2013). Auditing General and Application Controls.

Scarfone, Karen; Souppaya, M. (2013). NIST Special Publication 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise NIST Special Publication 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise, (June).

Schadler, T., & McCarthy, J. (2012). Mobile is the new face of engagement. *Forrester Research, February*. Retrieved from http://cdn.blog-sap.com/innovation/files/2012/08/SAP_Mobile_Is_The_New_Face_Of_Engagement.pdf

Stoel, M. D., & Muhanna, W. a. (2011). IT internal control weaknesses and firm performance: An organizational liability lens. *International Journal of Accounting Information Systems*, *12*(4), 280–304. doi:10.1016/j.accinf.2011.06.001

Stott, J. H., & Parker, X. L. (2002). Electronic Systems Assurance and Control.

Swanson, S., Astrich, C., & Robinson, M. (2012). Cyber Threat Indications & Warning: Predict, Identify and Counter. Retrieved from http://indianstrategicknowledgeonline.com/web/Small Wars Journal - Cyber Threat Indications.pdf

Thurner, R. (2010). Key Success Factor: IT Resource Management. *CoBiT Focus*, *2*(April).

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, *14*. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/1467-8551.00375/abstract

Trend Micro. (2012). Android Under Siege : Popularity Comes at a Price.

Umberger, H., & Gheorghe, A. (2011). Cyber Security: Threat Identification, Risk and Vulnerability Assessment, 247–269. doi:10.1007/978-94-007-0719-1

Unhelkar, B. (2010). The Enterprise Mobile Applications Development Framework, 33–39.

Verizon. (2012). 2012 Data Breach Investigations Report. *Zhurnal Eksperimental'noi I Teoreticheskoi Fiziki*. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+Title#0

Vodafone. (2010). Securing freedom : Minimising the risks of working without wires.

Wielstra, S. (2014). Assessing the impact of business process redesign decisions on internal control within banks.

Xu, L. Da. (2011). Enterprise systems: state-of-the-art and future trends. *Industrial Informatics, IEEE Transactions on*, *7*(4), 630–640. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6011699

Appendices

Appendix A ISO/IEC 27000 information assets categorization

Pure information assets	
Digital data	Personal, financial, legal, research and development, strategic and commercial, email, voicemail, databases, personal and shared drives, backup tapes/CDs/DVDs and digital archives, encryption keys
Tangible information assets	Personal, financial, legal, research and development, strategic and commercial, mail/post, FAXes, microfiche and other backup/archival materials, keys to safes/offices and other media storage containers, Journal, magazines, books
Intangible information assets	Knowledge, business relationships, trade secrets, licenses, patents, trademarks, accumulated experience and general know-how, corporate image/brand/commercial reputation/customer confidence, competitive advantage, ethics, productivity
Application software	In-house/custom-written systems, client software (including shared or single-user 'End User Computing' desktop applications), 'commercial off-the-shelf' (COTS), ERP, MIS, databases, software utilities/tools, eBusiness applications, middleware
Operating system software	For servers, desktops, mainfrafmes, network devices, handhelds and embedded systems (including BIOS and firmware)
Physical IT assets	
IT support infrastructure	IT buildings, data centers, server/computer rooms, LAN/wiring closets, offices, desks/drawers/filing cabinets, media storage rooms and safes, personnel identification and authentication/access control devices (turnstiles, card-access systems etc.) and other security devices (CCTV etc.)
IT environmental controls	Fire alarms/suppression/firefighting equipment, uninterruptible power supplies (UPSs), power and network feeds, power conditioners/filters/transient suppressors, air conditioners/chillers/alarms, water alarms
IT hardware	Computing and storage devices e.g. desktops, workstations, laptops, handhelds, servers, mainframes, modems and line terminators, communications devices (network nodes), printers/copiers/FAX machines and multifunction devices
IT service assets	
It service assets	User authentication services and user administration processes, hyperlinks, firewalls, proxy servers, network services, wireless services, anti-spam/virus/spyware, intrusion detection/prevention, teleworking, security, FTP, email/IM etc., Web services, software maintenance and support contracts
Human information assets	
Employees	Staff and managers, particularly those in key knowledge management roles such as senior/executive managers, software architects/developers/testers, systems managers, security administrators, operators, legal and regulatory compliance people, power users, local IT / IT security administrators and "go-to" people in general
Non-employees	Temporary workers, external consultants/specialist advisors, specialist contractors (e.g. those who understand maintenance of the physical IT environment), suppliers and business partners ...

Appendix B Mobile threat categorization

Threat/Vulnerability			Description	Risk	C	I	A	Area
Social engineering	Social network mining		The process of data mining to obtain personal employee information	Attackers gain personal information about specific employees, which they use in other social engineering methods	X			User
	Spear Phishing	Watering Hole Attack	The attacker wants to attack a particular group (organization, industry, or region). The attack consists of three phases: 1. Guess (or observe) which websites the group often uses. 2. Infect one or more of these websites with malware. 3. Eventually, some member of the targeted group will get infected.	Attackers gain personal information about specific employees that can possibly be used to gain unauthorized access to the enterprise system	X	X		User
		E-mail spoofing	An attacker sends one or a select group of employees an e-mail, which seems to come from a legit source, asking for information which can be used to gain unauthorized access to company systems.		X	X		User
	Pharming	Spoof websites	Collection of passwords through fake websites, which are tried on other accounts of employees like e-mail and web portals.	Attackers gain unauthorized access to parts of the system	X			NA
	Spoofing / identity theft		Pretending to be someone else and gain access to parts of the system (e.g. an attacker calls someone and pretends to be the secretary of a highly placed manager, who forgot his password and needs to know it)	Attackers gains unauthorized access to parts of the system	X			NA
	Doxing		Identifying someone's anonymous internet identity and using this to its advantage (e.g. blackmailing someone for statements this person gave on internet forums)	Attackers could blackmail employees into providing sensitive (personal) information	X			NA
	Drive-by-downloads		1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet). 2. Any download that happens without a person's knowledge, often a computer virus, spyware, malware, or crimeware.	Malicious software could be installed on devices of employees without them knowing it	X			Apps
(Web) Exploits	Software vulnerability		Vulnerabilities in software that can be used to distribute malware or hack into systems (e.g. browsers, cms, pdf readers and flash players might prove vulnerable)	Malicious software could be installed on the devices of employee without them knowing it	X			Device
	Zero-day attack		When vulnerabilities are found these are often published on the internet and usable for hackers against organizations who fail to address and patch vulnerabilities fast enough.	The enterprise system is not protected against the latest threats causing the system to be vulnerable to exploitation	X			Mobile platform, Device
	Information leakage		This threat is differentiated from data breaches, as it merely concerns technical or	Corporate information is leaked that is used by attackers	X			User

		organizational information that might be interesting for threat actors in order to perform reconnaissance and delivery of their attacks	for reconnaissance, prior to delivery of other attacks				
Code Injections	Cross-Site Scripting (XSS)	A type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy.	Attackers gain unauthorized access to parts of the system	X			Device
	Directory Traversal	Consists in exploiting insufficient security validation / sanitization of user-supplied input file names, so that characters representing "traverse to parent directory" are passed through to the file APIs. The goal of this attack is to order an application to access a computer file that is not intended to be accessible.	Attackers gain unauthorized access to parts of the system	X			Device
	SQL injection (SQLi)	A code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution	Attackers gain unauthorized access to parts of the system	X			Apps
	Cross-Site Request Forgery (CSRF)	A type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.	Attackers gain unauthorized access to parts of the system	X			Device
Encryption attacks	Transport Layer Security (TLS) Attacks	An attack on the encryption of TLS	Attackers gain unauthorized access to parts of the system	X	X		Data & network
	Brute Force Attack	Attackers use computer power to crack encryptions or passwords. To enlarge the capacity of this process, often botnets are used.	Attackers gain unauthorized access to part of the system	X	X		Data & network
	Secure Socket Layer (SSL) attacks	An attack on the encryption of the SSL	Attackers gain unauthorized access to parts of the system	X	X		Data & network
Malware	Rogueware/Ransomware/Scareware	Malicious software that locks your computer or system and asks for a ransom to release this lock. Other slightly different approaches might apply. Often when paid the virus does not disappear.	Employees are no longer able to access parts of the system	X		X	Apps
	Trojans	A non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm.	Information can potentially be lost, or stolen by attackers	X			Apps
	Worms	A standalone malware computer program that replicates itself in	Information can potentially be lost, or stolen by attackers		X		Apps

		order to spread to other computers.					
	Virus	A type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes.	System resources can become occupied, and information can be lost, stolen, or corrupted	X	X	X	Apps
	Spyware	Malicious software that copies/ steals data from an information system or device.	Information is copied from the system or device, now accessible to the attacker	X			Apps
	Exploit kits	These are ready-to-use software tools offering a large variety of functions, configuration options and automated means to launch attacks. Exploit kits search for vulnerabilities in order to abuse them and launch any applicable attack to take over an asset.	Method itself doesn't impact CIA of information, but allows for other methods (e.g. malware) to manifest themselves.				Apps
	(D)DoS	Once malware is installed this might be used to cause a denial of service	System resources become occupied, making the system no longer accessible			X	Data & network
	Direct billing	A method where a consumer pays by charging the purchase to the consumer's mobile phone.	Compromised devices can possible lead to unwanted billing to the employee's mobile phone	NA	NA	NA	Apps
	Location tracking	Tracking the location of the mobile device	When an attacker correlates an employee's location with other information, one can determine what sort of activities are performed, and with which clients	X			Device
	Sensitive Information Disclosure (SID)	Hardcoding sensitive information into application code	Once an attacker has sensitive information such as login credentials, shared secret keys, or access tokens, it is easy to access more sensitive data.	X			Apps
Insider attack	Thumb sucking	The name given to data theft using a USB mass storage device, such as a USB flash ("thumb") drive to download confidential network information, literally "sucking" the data out of the network and onto the USB drive. Could also be done with a mobile device.	Corporate data is mass-stored on the mobile device	X			User
	Pod-slurping	This involves using an iPod, MP3 type player, or mobile device to rapidly steal gigabytes of information from an enterprise's computer system.	Corporate data is mass-stored on the mobile device	X			User
	Espionage	Espionage is the covert act of spying through copying, reproducing, recording,	Corporate data is obtained by unauthorized employees	X			User

			photographing, interception, etc. to obtain information.					
	Employee abuse or fraud		Addresses authorized users who abuse their assigned access privileges or rights to gain additional information or privileges.	Authorized users use their access privileges to gain additional information or privileges that should not be authorized	X	X		User
	Impersonation	Physical access	Could include misuse of personal identification numbers (PIN)	An employee uses another employee's device to perform actions or obtain information that employee should not have access to	X	X		User
		Electronic system access	Could include use of others' authentication information in an attempt to gain system privileges and access to system resources	An employee uses another employee's device to perform actions or obtain information that employee should not have access to	X	X		User
	Misuse of known software weaknesses or procedures		Deliberate act of bypassing security controls for the purpose of gaining additional information or privileges.	Employees bypass security controls to gain additional information or privileges	X			User
Insider error	UPnP		Universal Plug and Play (factory) configurations of devices can prove to be unsafe.	Attackers could gain system access due to improper UPnP configurations	X			Control procedures
	Procedural violation		The act of accidently not following standard instructions or procedures	Employees not aware of certain procedures might fail to adhere to them, potentially causing information leakage or entry of incorrect data	X	X		User
	Accidental data breach		A threat that can materialize due to errors and mistakes of personnel, resulting in data loss.	Corporate data is leaked to another party or to the public	X			User
Device vulnerabilities	(offline) tampering		An unauthorized modification that alters the proper functioning of equipment in a manner that degrades the security functionality the asset provides	Security functionalities of the mobile device are degraded due to tampering of the device	X	X	X	User
	Misuse of Phone Identifiers							NA
	Technical failure of device		Unexpected loss of operational functionality of the mobile device	Employee is no longer able to use the device, and thus access the system			X	Device
Technical threats	Eavesdropping		The deliberate attempt to gain knowledge of protected information.	Potentially sensitive corporate data can be disclosed by other parties	X			Data & network
	No proper auditing and logging		Lack of sufficient auditing and logging of system and application errors failures, and intrusions reduced administrators' capabilities to troubleshoot and safeguard performance issues, and reconstruct events of unauthorized access.	Events of unauthorized access can be hard to identify, and performance difficult to ensure		X		Control processes
	Electromagnetic Interference (EMI)		The impact of signal transmitters and receivers operating in proximity to the device, which could cause an interruption in its operational use.	Operational use of the mobile device becomes less available			X	Environment
	Compromising emanations		The data-related or intelligence-bearing signals, which, if intercepted and analyzed, could disclose sensitive information being transmitted and/or processed	Corporate data can be exposed and intercepted by an attacker	X			Environment
	Data/system contamination		The intermixing of data of different sensitivity levels, which could lead to an accidental or intentional violation of data integrity	Data of different sensitivity levels is mixed meaning that violation of data integrity could be impaired		X		Data & network
	Hazardous material accident		The unexpected spill of material on the device, that causes damage to it.	The mobile device gets damaged and becomes			X	Environment

Environmental			unusable to the user, meaning the system is inaccessible				
	Shoulder surfing	The deliberate attempt to gain knowledge of protected information from observation.	Potentially sensitive information is obtained by the attacker	X			Environment, User
	Unauthorized physical device access	Others than the primary user of the device has access to the mobile device	Unauthorized persons can access and possibly change corporate data	X	X		Environment, User

Appendix C Controls overview

NIST 800-124	
Device	
Authentication	Require authentication before gaining access to the mobile device or organization's resources accessible through the device (generally there is one user per device, which means no username is used. Often a PIN is used, yet more robust forms of authentication such as token-based authentication can be used)
Data encryption	Protect sensitive data, either by encrypting mobile device's storage, or not storing sensitive data on mobile devices.
Sandboxing	Implore technical solutions for achieving degrees of trust in BYOD devices, such as running organization's software in a secure, isolated sandbox/secure container on the mobile device, or using device integrity scanning applications
Prohibit/restrict	Possibly restrict or prohibit the use of BYOD devices, favoring organization-issued devices.
Monitor	Fully secure each organization-issued mobile device, getting it in an as-trusted state as possible. Deviations from this secure state can be monitored and addressed.
User	
Awareness	Train users on awareness to reduce frequency of insecure physical security practices
QR readers	Have applications such as QR readers display the un-obfuscated content (e.g. the URL, and allow users to accept or reject it before proceeding
Location services	Train users to turn off location services when in sensitive areas
Data & network	
Network encryption	Use strong encryption technologies (such as VPNs)
Mutual authentication	Use mutual authentication mechanisms to verify identities of both endpoints before transmitting data
Insecure Wi-Fi	Prohibit the use of insecure Wi-Fi networks (those running known vulnerable protocols)
Network interfaces	Disable all network interfaces not needed by the device, reducing the attack surface
Application	
Third-party apps	Possibly prohibit all installation of third-party applications
Whitelisting	Implement whitelisting to allow installation of approved applications only
Permissions	Verify applications only receive necessary permission on the device
Risk assessment	Perform a risk assessment on each third-party application before permitting its use on the organization's mobile device
Location services	Prohibit use of location services for particular applications (social networking or photo applications)
Web-browser	
Prohibit/restrict	Prohibiting or restricting browser access;
Force traffic	Forcing mobile device traffic through secure web gateways, HTTP proxy servers, or other intermediate devices to assess URLs before allowing them to be contacted
Separate browsers	Using a separate browser within a secure sandbox for all browser-based access related to the organization, leaving the mobile device's built-in browser for other uses
Environment	
Restrict	Restrict what devices a mobile device can synchronize with (organization-issued mobile device).
Remote back-up	Blocking use of remote back-up services, or configuring mobile devices not to use remote back-up services
Instruct users	Instruct users not to connect their mobile device to unknown charging devices

NOREA	
Access to device	Password/PIN code/other security measure required for accessing the device
Device security activation	Automatically activate security of device as soon as possible, even though users may find this annoying in practice, because inactive security is useless
Remote wipe	Or remote blocking of the device
Device environment	Do not lend a mobile device to others, such as children or partners
Encryption	Consider using encryption for valuable information
Security software	Consider using security software on your mobile device
Software updates	Ensure software is update as soon as possible to its most recent version
Information storage	Try not to store sensitive information on your mobile device, and delete information if it is nog longer needed
Secure data connections	Use secured data connections (TLS encryption for email, HTTPS for web/VPN connections)
Connection methods	Turn off WiFi/Bluetooth connections when leaving your device somewhere, or when they are simply not needed
Public networks	Do not randomly connect to open networks in public areas
Lost/stolen device	Develop a documented procedure that specifies what to do when a device is lost or stolen, including the services that need to be disconnected
Apps	Be critical with choosing which apps to install on your device

Appendix D Interview protocols

Appendix D.1 Interview protocol Suppliers & Consultants

Introduction

1. What is your current function?
2. What is your background related to mobile and/or ERP solutions?

Strategy & usage

3. If you look at the current market, for what purposes are M-ERP solution mostly used?
    a. Which business processes are mostly supported with M-ERP?
    b. Which IT processes are mostly supported with M-ERP? (change management)
4. Do these processes process sensitive information?
    a. To what extent is sensitive information being disclosed via the mobile device?
    b. To what extent is information being stored on the mobile device?
5. What type of clients are typically found on mobile devices?
    a. Standalone applications
    b. Smart/full clients
    c. Thin clients
6. Which strategies do you think are used most often?
    a. Why?

Risks

7. If you look at these attention areas, do you think they cover the full scope of risks related to ERP mobility?
    a. If not, what is missing? What should be different?

----- **Per attention area** -----

Risks & controls

8. What are the most important risks related to this area, to enterprises adopting ERP mobility?
    a. Which are most common?
9. Would you say the supported business processes that is supported with mobility affect the involved risks?
    a. How?
    b. To what extent?
10. Based on the aforementioned risks, what do you consider the most essential control activities, processes, procedures that need to be covered, to mitigate these risks?

----- **End sub-section** -----

Wrap-up

11. How do you see the concept of M-ERP solutions develop over the next coming years?
12. In terms of identifying risks affecting the CIA of information, do you think I missed any important areas during this interview?
    a. Which?
13. What do you think of the M-ERP risk-control framework concept?
    a. Are there any important concepts missing?
14. Are you aware of other persons and/or documentation that could be helpful for my research?

Appendix D.2 Interview protocol Organizations using ERP mobility

Introduction

1. What is your current function?
2. What is your background related to mobile and/or ERP solutions?

Strategy & usage

3. In your organization, for what purposes are is ERP mobility mostly used?
    a. Which business processes are supported with ERP mobility?
    b. Which IT processes are mostly supported with ERP mobility?
4. Do these processes process sensitive information?
    a. To what extent is sensitive information being disclosed via the mobile device?
    b. To what extent is information being stored on the mobile device?
5. What type of clients do you use on mobile devices?
    a. Standalone applications
    b. Smart/full clients
    c. Thin clients
6. Which strategies do you think are used most often?
    a. Why?

Risks

7. If you look at these attention areas, do you think they cover the full scope of risks related to ERP mobility?
    a. If not, what is missing? What should be different?

----- Per business process supported with ERP mobility -----

Risks & controls

8. What are the steps in this process where communication takes place with the mobile device?
    a. In each step of the process, what are the risks that could impact the CIA of information?
9. Based on the aforementioned risks, what do you consider the most essential control activities, processes, procedures that need to be covered, to mitigate these risks?

----- End sub-section -----

Wrap-up

10. How do you see the concept of M-ERP solutions develop over the next coming years?
11. In terms of identifying risks affecting the CIA of information, do you think I missed any important areas during this interview?
    a. Which?
12. What do you think of the M-ERP risk-control framework concept?
    a. Are there any important concepts missing?
13. Are you aware of other persons and/or documentation that could be helpful for my research?

Appendix E Preliminary Risk-Control Framework

M-ERP RISK-CONTROL FRAMEWORK – INITIAL CONCEPT						
ID	**AREA**	**RISK**	**DESCRIPTION**	**ID**	**CONTROL**	**DESCRIPTION**
1	**Policy**	Lack of mobile-related policy	Due to a lack of regulations set in policy, the likelihood of other risks occurring is severely increased.	1.1	Mobile Policy	Implement a policy with regulations to which employees should live by, avoiding potential risks.
				1.2	App development guidelines	Define development guidelines for in-house development of apps.
2	**Apps**	Use of untrusted applications	Apps could track and expose location, abuse resources, or leak corporate information.	2.1	Secure container/ Sandboxing	Only from within the secure container access can be established to the corporate network, at which point synchronization takes place.
				2.2	Selective management	Adopt a form of selective management, to separate business apps from personal apps.
3	**Apps**	Malware	Malicious software that performs unwanted, unauthorized activities (e.g. worms, Trojans, viruses).	3.1	Whitelisting	Implement whitelisting to allow installation of approved apps only. Apps can get on the whitelist after a screening process.
				3.2	Blacklisting	Implement blacklisting to restrict installation of identified apps that are deemed malicious. Apps can get on the blacklist after a screening process.
4	**Apps**	Reverse Engineering	Hardcoding information into application code means that an attacker might be able to access such information through reverse engineering.	4.1	App development guidelines	Refer to 1.2.
5	**Apps**	Data leakage through unauthorized/insecure/malicious applications	Applications that are not authorized to be installed can potentially be insufficiently secure, or contain malicious software.	5.1	Whitelisting	Refer to 3.1.
6	**Data & network**	Uncontrolled external storage	Usage of mobile devices stimulates employees to store information on external locations (such as cloud services), of which the organization has no control over.	6.1	Remote desktop	Access and store data remotely, without storing data on the device.
				6.2	Restrict access to external storage	Restrict access to external location (cloud services such as Dropbox) from within the corporate network, and from the mobile device.
				6.3	User awareness training	Educate employees on the risks of storing information on remote (cloud) locations.
7	**Data & network**	Eavesdropping or modifying network traffic	The deliberate attempt to gain knowledge of protected information, through which potentially sensitive data can be disclosed by other parties.	7.1	Secure network connectivity	Ensure the connection between the mobile device and back-end enterprise system is secure.
8	**Data & network**	Leaking of data	Extraction or loss of valuable information.	8.1	Encrypt data and network connections	For instance with RSA public/private key encryption.
9	**Data & network**	Unauthorized access to internal network	Attacks gain unauthorized access to (parts of) the system.	9.1	Encrypt data and network connections	For instance with RSA public/private key encryption.
10	**Data & network**	Data contamination	Data of different sensitivity levels are mixed, meaning that data integrity could be impaired (e.g. WhatsApp pulls all persons from your contact list).	10.1	Secure container	Refer to 2.1.

11	**Data & network**	Personal versus corporate data	Storing both private and corporate data on the same device potentially mixes the two, blurring the line between sensitive corporate data and other data.	11.1	Secure container	Refer to 2.1.
				11.2	Selective management	Refer to 2.2.
12	**Data & network**	Use of location services	Enables other parties to relate location-based information to other information, potentially finding out the kind of activities or clients a user is associated with.	12.1	Prohibit or restrict usage of location services	Prohibit or restrict usage of location services in documented procedures so that if other risks manifest themselves, location-based information cannot be misused.
13	**Data & network**	Use of untrusted networks	Untrusted open Wi-Fi networks might use vulnerable protocols and should therefore not be trusted.	13.1	User awareness training (public networks)	Educate employees on the risks involved with using public networks.
				13.2	Always-on VPN	Implement always-on VPN protocol, increasing the security of the connection between mobile device and back-end enterprise system.
14	**Data & network**	Replay attack	Form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.	14.1	Session tokens	When mobile devices connect to the enterprise system, require these connections to use session tokens.
				14.2	One-time passwords	When mobile devices connect to the enterprise system, verify these connections are valid by sending one-time passwords that are unique for every connection being established.
15	**Data & network**	Spoofing	Situation in which one person or program masquerades as another by falsifying data and thereby gaining illegitimate advantage.	15.1	User awareness training (spoofing)	Educate employees on the risks of spoofing activities, and how to identify such attacks.
16	**Data & network**	Man-in-the-middle attack	For instance through hotspot architectures that do not use any form of encryption.	16.1	Encrypt data	Encrypt data.
17	**Data & network**	Insecure data storage	Insecure data storage could potentially lead to loss of sensitive corporate data.	17.1	Mobile data protection program	Implement a centrally managed mobile data protection program, including data classification, encryption techniques, and legal requirements. Confirm that local data storage has a business need. If not, data should not be stored on the device.
18	**Data & network**	Improper Bluetooth operations configuration	Enables direct communication, including sharing of content, between mobile devices.	18.1	Pre-configuration	Pre-configure or configure mobile devices with MDM solution so that Bluetooth settings are properly configured.
19	**Control P&P**	Lack of auditing and logging	Events of unauthorized access can be hard to identify, and performance difficult to ensure.	19.1	Audit Logging	Maintain an audit log of events and activities performed on mobile devices as part of a MDM solution.
20	**Control P&P**	Insufficient OS/app version control	Mobile operating systems that are not up-to-date with the latest version have a chance of not being up-to-par with latest security changes.	20.1	OS version control	Implement a MDM solution that can monitor devices and check if mobile operating systems being used are sufficient. If not, access to the enterprise system should not be allowed.
21	**Users**	Social engineering / (Spear) Phishing	Attackers gain personal information about specific employees that can be used to gain unauthorized access to the enterprise system. Due to smaller screen and less awareness of information security this is amplified on mobile devices.	21.1	User awareness training (social engineering)	Educate users on the risks of social engineering activities, and how to identify such attacks.
22	**Users**	Use of untrusted content	Mobile device are able to process content other devices typically do not, such as QR-codes that could potentially lead to malicious destinations.	22.1	User awareness training (mobile content)	Educate users on the risks of using untrusted and unknown content.

23	**Users**	Pharming	Technique used to direct the unsuspecting victim to a malicious website, where a network node is hijacked and all traffic passing the node will be redirected.	23.1	User awareness training (pharming)	Educate users on the risks of pharming activities, and how to identify such attacks.
24	**Users**	Espionage	Covert act of spying through, copying, reproducing, recording, photographing, intercepting, to obtain information.	24.1	Screen privacy protector	Implement usage of foils over tablet screens to reduce the possibility of others being able to read information from the device.
25	**Users**	Data entry errors or omissions	Mistakes in keying or oversight to key data.	25.1	No control	-
26	**Users**	Misuse	Employees bypass security controls to gain additional information or privileges.	26.1	Open policy	Don't restrict everything related to using mobile devices tightly down, by not allowing employees any freedom. This tends to be counterproductive in terms of securing mobile devices because employees will feel they miss out on things, stimulating them to search for workarounds of security mechanisms that are in place.
27	**Users**	Insider error	Employees (accidently) fail to adhere to procedures or policy causing information leakage or incorrect data entry.	27.1	User awareness training (corporate policy)	Educate employees on how to properly use their mobile devices, so that the risks of accidental errors can be minimized.
28	**Users**	Impersonation	An employee uses another employee's device to perform actions he/she should not be able to.	28.1	User awareness training (corporate policy)	Educate employees on the risks of lending personal mobile device to other employees.
29	**Users**	Device tampering	Security functionalities of the mobile device are degraded due to tampering of the device by the employee.	29.1	User awareness training (root access)	Educate employees on the risks of tampering with their mobile device (Jail breaking and Root access).
30	**Users**	Fraud	Authorized users use their access privileges to gain additional information or privileges that should not be authorized.	30.1	Segregation of Duties	Implement a proper segregation of duties so that employees won't be able to gain additional privileges, in addition to their already assigned privileges. This can be done with standard back-end ERP tools, creating every mobile device user on the server.
31	**Device**	Careless decommissioning of device	If a mobile device must be decommissioned it must not contain any corporate information anymore. Employees are however often not aware of having stored corporate information on their mobile device, making successful decommissioning less self-evident.	31.1	Mobile Device Decommissioning	Remote device wipe, reset, kill, lock functionalities. Also, remove configuration data, wipe encrypted and application data.
32	**Device**	Lack of physical security	If no physical security measures are implemented the risk of losing a mobile device is significantly increased, because a third party will have full access to the device.	32.1	Passwords, recovery configurations	Implement password and recovery configurations, requiring employees to use a form of authentication to gain access to the device.
33	**Device**	Use of untrusted devices in BYOD environments	If any device may be brought into the corporate network devices may not be up-to-par with latest security mechanisms.	33.1	CYOD	Implement a Choose- Your-Own-Device strategy where employees can pick from a pre-selected list of approved mobile devices that have been screened; and only support those devices that are pre-approved.

34	**Device**	Loss/theft	Lost or stolen devices grants the attacker access to anything stored on the device.	34.1	Procedure lost/stolen device	Implement a documented procedure for employees, stating the steps they should take in case their mobile device gets lost or stolen.
				34.2	Remote wipe	Implement a MDM solution through which administrators are able to remotely wipe (parts of) data stored on the mobile device.
35	**Device**	Pod slurping	Using a mobile device to download confidential data onto their device, for instance performed by employees inside the organization.	35.1	User awareness training (local data)	Educate users on the risks of storing data locally on a mobile device, and stimulate them to store as little as possible data on their mobile device
36	**Device**	Technical failure of device or operating system	Unexpected loss of operational functionality of the device, meaning that the employee is no longer able to use the device and thus the system.	36.1	Recovery	Enable recovery of data on mobile devices should they no longer be accessible.
37	**Device**	Operating system flaws	Any flaws in the operating system used on corporate mobile devices also affect the system to which these devices have access to.	37.1	No control	-
38	**Device**	Browser exploitation	Vulnerabilities in the web-browser used on mobile devices may be exploited. These are often less considered on mobile devices because users are often less aware of risks when using mobile devices, and smaller sized screens cause security characteristics (such as the "s" in "https") to be less obvious.	38.1	Secure container	Refer to 2.1.
39	**Environment**	Shoulder surfing	The deliberate attempt to gain knowledge of protected information through observation, through which potentially sensitive data can be disclosed by other parties.	39.1	Screen privacy protector	Implement usage of foils over tablet screens to reduce the possibility of others being able to read information from the device.
				39.2	User awareness training (shoulder surfing)	Educate users on the risks of shoulder surfing in a document user awareness program.
40	**Environment**	Sharing of device	Sharing of device increases the risk of unauthorized access, especially with regard to tablets because of their nature (larger screen, accessibility).	40.1	Security apps	Implement apps that secure specific folders on the device with some sort of authentication.
				40.2	Secure container	Refer to 2.1.
				40.3	Separate authentication	Require the user of a mobile device to authenticate him-/herself when using specific business apps on installed on the device that process potentially sensitive corporate information.
41	**Environment**	Interaction with other (untrusted) systems	If a mobile device connects to another system (such as a desktop or laptop computer), information may be stored on other systems, creating a copy of potentially sensitive information on an unsecured device.	41.1	Secure container	Refer to 2.1.
				41.2	Restrict access to other systems	Do not allow mobile devices to connect to other systems, such as desktop computers, laptops, or other storage devices).
42	**Mobile Platform**	Diversity of mobile platforms	Each platform supports its own security measures, requiring different additional security measures to be set by the organization.	42.1	Control procedure	Develop protocols in an established policy for additional security measures that need to be in place for the mobile operating systems that are being used in the organization.

Appendix F Final M-ERP Control Framework (M-ERP CF)

Control area	Control	Description
Mobile data protection program	Data classification	A documented centrally managed data classification is defined, stating what data may be accessed by whom through mobile devices. A classification of data can be made based on the value of each set of data, for instance in terms of the type and sensitivity of data. Data should be processed, stored, and used according to this classification.
	User awareness program	A documented user awareness program is defined, including data management risks, network connectivity risks, common cyber threats, tips, and best practices related to ERP mobility.
	Mobile device corporate policy	A mobile device corporate policy is defined including at least: * Lost/stolen procedure - A procedure is defined for employees in case of a lost or stolen devices. * User authentication – A policy is defined that states user authentication is always required, and additional user authentication is required for high-profile business apps. * Remote functionalities – A policy is defined that states when and which remote functionalities are to be used through MDM capabilities, for instance in case of mobile devices being rooted. * Privacy: A policy is defined that covers the usage of personal information being stored and transferred on and through mobile devices.
Device configuration	Policy configuration	Mobile devices are configured according to corporate policy. Events related to bypassing mobile device configurations by employees are monitored as described in control 4.3.
	Security tools	Mobile devices are pre-installed with security tools that scan apps for vulnerabilities, including antivirus software.
	Secure containers	Secure containers/sandboxing implementations are used to ensure a separation of apps and their related data.
	User authentication	With regard to user authentication being required before granting access to the device the following implemented: * PIN numbers of more than 4 characters are allowed if possible with the mobile OS. * Repeated patterns for swipe-based visual passwords are allowed if possible with the mobile OS. * Passwords and keys are not visible in any cache or logs. * Generic shared secret for integration with the back-end application are not used.

Control area	Control	Description
		* Multi-factor authentication is implemented for high-profile apps processing sensitive data, based on the data classification.
Mobile asset management	White- and blacklists	Documented white- and blacklists of apps are defined to grant insight in apps that should not be trusted. Before apps are included in either list they are subject to a screening process. Whitelisted apps are kept track of to identify required security updates.
	App development	Documented app development guidelines are defined if a development platform is used including and incorporating the following: * The principle of minimal disclosure is applied by only collecting and disclosing data that is actually required by the app. * Application-specific data-wipe capabilities with strong user-authentication are provided for apps that process sensitive data. * Apps are only distributed via official app stores and provide feedback mechanisms that employees can use in case of security issues. * Input validation is implemented to ensure input is valid. Input whitelists, blacklists, or filtering may be used, also referred to as input sanitization. * Apps are developed so that they do not store data beyond the period required by the app.
	App expiration duration	A mechanism is implemented to ensure that the user is logged out of business apps after a defined time of inactivity.
	App monitoring	Apps on issued mobile devices are monitored in terms of updates that should be installed, and pushed to all devices when needed.
	Lockout recovery	Data can be recovered from mobile devices that have previously been locked in case the lockout is no longer required.
Mobile device management	Remote functionalities	Remote functionalities such as device wipe/reset/kill/lock are used according to corporate policy.
	Monitoring	The following events are monitored: * Audit log – An audit log of events and activities related to corporate data that are performed on mobile devices is maintained. * The back-end keeps track of events triggered by mobile devices in terms of completed and attempted access requests to data, and retains a log of this. * OS version control - Mobile devices are monitored in terms of operating system versions, and push updates when available and validated. * Root detection – A solution is implemented that allows detection of mobile devices becoming rooted.

Control area	Control	Description
		In case of such an event, procedures are initiated as defined in corporate policy.
	Geo-fencing	For apps that may only be accessed in certain locations, access to data or apps is restricted based on the mobile device's geographical location.
Data & network security	External cloud services	Access to external cloud services such as Google Drive, Dropbox, and OneDrive is restricted.
	Secure connection – end-to-end channel	With regard to the connection between mobile device and back-end application, ensure a secure end-to-end channel is implemented such as SSL or TLS.
	Secure connection – certificate usage	With regard to the connection between mobile device and back-end application, digital certificates signed by a trusted certificate authority are used. Furthermore, establishment of a connection is only granted after verification of the identity of the remote end-point- by ensuring they have a trusted certificate.
	Secure connection – VPN	With regard to the connection between mobile device and back-end application, a dedicated VPN connection is used.
	Secure connection – unique session	To further secure the connection between mobile device and back-end application the following is implemented: * session tokens * one-time passwords * multi-factor authentication
	Data in transit	With regard to data being transferred over the connection between mobile device and back-end application, the following is ensured: * Data transmitted over the connection between the mobile device and the back-end application is encrypted with AES. * SMS, MMS, or notifications are not used to send sensitive information. In addition, periodically a check is performed to see if sensitive data is unintentionally transferred to mobile devices, such as location information being included as meta-data.
	Data access and storage	With regard to data access and stored, the following is ensured: * Sensitive data is stored on the server and not the mobile device. * Files that are locally stored on the mobile device are encrypted. * Shared storage services are considered as untrusted, a matter which is included in user awareness programs.

Control area	Control	Description
		* A maximum retention periods is defined based on which sensitive personal data automatically gets deleted. * Control is enforced on who can access and store data through/on mobile devices, in consensus with the mobile data classification defined in the mobile data protection program.

Appendix G Dashboard screenshots

Appendix G.1 Screenshot Risk Assessment

ERP mobility risk overview

ID	Risk	Description
1	Lack of mobile-related policy	Due to a lack of regulations set in policy, the likelihood of other risks occurring is severely increased.
2	Use of untrusted applications	Apps could track and expose location, abuse resources, or leak corporate information.
3	Malware	Malicious software that performs unwanted, unauthorized activities (e.g. worms, Trojans, viruses).
4	Reverse Engineering	Hardcoding information into application code means that an attacker might be able to access such information through reverse engineering.
5	Data leakage through unauthorized/insecure/malicious applications	Applications that are not authorized to be installed can potentially be insufficiently secure, or contain malicious software.
6	Uncontrolled external storage	Usage of mobile devices stimulates employees to store information on external locations (such as cloud services), of which the organization has no control over.
7	Eavesdropping or modifying network traffic	The deliberate attempt to gain knowledge of protected information, through which potentially sensitive data can be disclosed by other parties.
8	Leaking of data	Extraction or loss of valuable information.
9	Unauthorized access to internal network	Attacks gain unauthorized access to (parts of) the system.
10	Data contamination	Data of different sensitivity levels are mixed, meaning that data integrity could be impaired (e.g. WhatsApp pulls all persons from your contact list).
11	Personal versus corporate data	Storing both private and corporate data on the same device potentially mixes the two, blurring the line between sensitive corporate data and other data.
12	Use of location services	Enables other parties to relate location-based information to other information, potentially finding out the kind of activities or clients a user is associated with.
13	Use of untrusted networks	Untrusted open Wi-Fi networks might use vulnerable protocols and should therefore not be trusted.
14	Replay attack	Form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.
15	Spoofing	Situation in which one person or program masquerades as another by falsifying data and thereby gaining illegitimate advantage.
16	Man-in-the-middle attack	For instance through hotspot architectures that do not use any form of encryption.
17	Insecure data storage	Insecure data storage could potentially lead to loss of sensitive corporate data.
18	Improper Bluetooth operations configuration	Enables direct communication, including sharing of content, between mobile devices.
19	Lack of auditing and logging	Events of unauthorized access can be hard to identify, and performance difficult to ensure.
20	Insufficient OS version control	Mobile operating systems that are not up-to-date with the latest version have a chance of not being up-to-par with latest security changes.
21	Social engineering / (Spear) Phishing	Attackers gain personal information about specific employees that can be used to gain unauthorized access to the enterprise system. Due to smaller screen and less awareness of information security this is amplified on mobile devices.
22	Use of untrusted content	Mobile device are able to process content other devices typically do not, such as QR-codes that could potentially lead to malicious destinations.
23	Pharming	Technique used to direct the unsuspecting victim to a malicious website, where a network node is hijacked and all traffic passing the node will be redirected.
24	Espionage	Covert act of spying through, copying, reproducing, recording, photographing, intercepting, to obtain information.
25	Data entry errors or omissions	Mistakes in keying or oversight to key data.
26	Misuse	Employees bypass security controls to gain additional information or privileges.
27	Insider error	Employees (accidently) fail to adhere to procedures or policy causing information leakage or incorrect data entry.
28	Impersonation	An employee uses another employee's device to perform actions he/she should not be able to.
29	Device tampering	Security functionalities of the mobile device are degraded due to tampering of the device by the employee.
30	Fraud	Authorized users use their access privileges to gain additional information or privileges that should not be authorized.
31	Careless decommissioning of device	If a mobile device must be decommissioned it must not contain any corporate information anymore. Employees are however often not aware of having stored corporate information on their mobile device, making successful decommissioning less self-evident.
32	Lack of physical security	If no physical security measures are implemented the risk of losing a mobile device is significantly increased, because a third party will have full access to the device.
33	Use of untrusted devices in BYOD environments	If any device may be brought into the corporate network devices may not be up-to-par with latest security mechanisms.
34	Loss/theft	Lost or stolen devices grants the attacker access to anything stored on the device.
35	Pod slurping	Using a mobile device to download confidential data onto their device, for instance performed by employees inside the organization.
36	Technical failure of device or operating system	Unexpected loss of operational functionality of the device, meaning that the employee is no longer able to use the device and thus the system.
37	Operating system flaws	Any flaws in the operating system used on corporate mobile devices also affect the system to which these devices have access to.
38	Browser exploitation	Vulnerabilities in the web-browser used on mobile devices may be exploited. These are often less considered on mobile devices because users are often less aware of risks when using mobile devices, and smaller sized screens cause security characteristics (such as the "s" in "https") to be less obvious.
39	Shoulder surfing	The deliberate attempt to gain knowledge of protected information through observation, through which potentially sensitive data can be disclosed by other parties.
40	Sharing of device	Sharing of device increases the risk of unauthorized access, especially with regard to tablets because of their nature (larger screen, accessibility).
41	Interaction with other (untrusted) systems	If a mobile device connects to another system (such as a desktop or laptop computer), information may be stored on other systems, creating a copy of potentially sensitive
42	Diversity of mobile platforms	Each platform supports its own security measures, requiring different additional security measures to be set by the organization.

Appendix G.2 Screenshot M-ERP CF

Framework for improving ERP mobility related Internal Controls

This sheet provides an overview of controls that mitigate risks arising from mobility

ID	Risk summary	Control area	Area description	ID	Control	Description	Testing procedure
10, 17	Data of different sensitivity levels get mixed, users have access to data they should not have access to.	1. Mobile data protection program	The mobile data protection program control area contains three controls that together represent all policies and procedures to be set by an organization that relate to ERP mobility.	1.1	Data classification	Define and document a centrally managed data classification that may be accessed through mobile devices. Data should be processed, stored, and used in accordance with this classification.	Verify a document is defined that specifies a centrally managed data classification: 1. Verify a data classification document is available and up to date 2. Verify the data classification is used to determine who can access what type(s) of data
,13, 15, , 22, 23, , 27, 28, , 35, 33	Employees will lose their device, try to gain root access to their device, download untrusted content, or do not comply to corporate policy.			1.2	User awareness program	Define a user awareness program including data management risk, network connectivity risks, common cyber threats, tips, and best practices.	Verify a document is defined that specifies elements in a user awaress program, including common ERP mobility risks, network connectivity risks, common cyber threats, tips, and best practices. Furthermore verify elements including in the user awareness program are communicated to employees on a continuous basis.
24, 34,	Responsibility of data and devices in case of data/device loss is hard to determine, especially in BYOD environments. Without defined procedures, employees have no guidelines related to mobile device usage. Moreover a lack of mobile-related policy increases the likelihood of other risks occurring.			1.3	Mobile device corporate policy	* Lost/stolen procedure - Define a procedure for employees in case of a lost or stolen device. * User authentication - Define policy that states user authentication is always required, and separate user authentication is required for high-profile business apps. * Define policy on when and which remote functionalities are to be used through MDM capabilities * Define a privacy policy that covers the usage of personal information being stored and transferred on and through the device. * Screen privacy protector * Restrict connecting with external hardware	Verify a document is defined that specifies a mobile device corporate policy, including statements and procedures regarding the following: 1. Lost and/or stolen devices 2. User authentication 3. Remote MDM functionalities 4. Privacy 5. Screen privacy protectors 6. Connecting with external hardware
, 41	Though many security mechanisms and features on mobile devices exist, they are often not enabled my default nor mandatory, so that employees are forced to use them. This could mean	2. Device configuration	The device configuration control area consists of four controls that all relate to technical configuration of the mobile device before it is commissioned to an employee (pre-configuration) and involves controls that specify how a device should be configured.	2.1	Policy configuration	Preconfigure mobile devices according to policy.	Verify mobile devices are configured according to corporate policy before they are issued to employees: 1. Check availability and extent of corporate policy (control 1.3) 2. Verify compliance between device configuration and corporate policy
40	Viruses or other types of malware may try to affect a mobile device and steal or modify data.			2.2	Security tools	Pre-install mobile device security tools that scan apps for vulnerabilities, including antivirus software.	Verify mobile devices have require security tools available: 1. Check if security tools that scan apps for vulnerabilities 2. Check if antivirus software is present
,11, 33 , 40, 41	Attacks on a particular app that has access to other apps grants the attacker access to more data than just the original app itself. Furthermore private and corporate data can get intertwined with each other.			2.3	Secure containers	Implement secure containers/sandboxing to ensure separation of apps and their data.	Go through system configuration settings and verify communication between sandboxed apps and apps outside the sandboxed environment is restricted.
, 40	Should unauthorized individuals gain knowledge of the user's authentication mechanism they can use this to access resources stored on or accessed via the device.			2.4	User authentication	Require user authentication before granting access to the device: * Allow PIN numbers of 5 or more characters if possible with the mobile OS * Allow repeated patterns for swipe-based visual passwords * Ensure passwords and keys are not visible in cache or logs * Do not use a generic shared secret for integration with the back-end * Use multi-factor authentication for high-profile apps	Verify user authentication is required as defined in corporate policy: 1. Verify authentication process on a mobile device 2. Verify authentication process for high-profile business apps 3. Attempt to remove user authentication from the device
	Employees store a lot of personal rather than corporate data on their device. Infringing of this data may lead to employee dissatisfaction stimulating them to find work-arounds other than those provided by the organization.	3. Mobile Asset Management (MAM)	Mobile asset management (MAM) is about ensuring all assets on the mobile device are secure and managed properly, and consists of five distinct controls that mostly relate to managing apps and maintaining their integrity.	3.1	Selective management	Implement selective management to separate business and personal apps and data on the device in case employees are allowed to use their personally owned mobile devices.	Verify MDM capabilities related to selective management. Verify remote capabilities are restricted to corporate data and apps only.
3	Many apps that can be downloaded by employees contain malicious software designed to steal or modify data, potentially of sensitive nature. Apps could also track and expose the device's location and abuse its resources, or simply be			3.2	White- and blacklists	Define and enforce white- and blacklisting of apps, to have clear insight in apps that should not be trusted. Screen apps before adding them to the whitelist, and track apps for security updates.	Verify usage of white- and blacklists for apps: 1. Verify if whitelists are available 2. Verify if blacklists are available 3. Verify if an app verification process is available, and documented when used
	Poorly designed apps may enable attackers to reverse engineer app-code to obtain data, store sensitive information in application code, or otherwise enable retrieval of sensitive information.			3.3	App development	Define app development guidelines if a development platform is used: * Apply the principle of minimal disclosure by only collecting and disclosing data that is actually required by the app * Possibly include application-specific data-wipe capabilities with strong user-authentication * Only distribute apps via official app stores and provide feedback mechanisms that employees can use in case of security problems * Apply some sort of input validation	Verify if documented app development guidelinenes are defined: 1. Check availability of a defined app developments guidelines document 2. Check adherence to guidelines in application code
:	If apps are automatically accessible to the user all the time the chance of unauthorized access is increased.			3.4	App expiration duration	Implement a mechanism so that the user is logged out of business apps after a defined amount of inactivity.	Verify users are logged out of business apps after a defined time of inactivity: 1. Check app configurations for app expiration durations 2. Check app code for app expiration durations
	App updates may impose changes in terms of access or data storage requirements that are not desirable.			3.5	App monitoring	Monitor apps on devices in terms of updates that should be installed, and push updates to all devices when needed.	Verify a system is implemented that monitors apps for updates: 1. Verify such a system is implemented and active 2. Verify that when updates are found and validated they are pushed to eligible devices
, 32, 34	Mobile device may get lost, stolen, or otherwise compromised, resulting in unauthorized parties having access to its resources.			4.1	Remote functionalities	Use remote device wipe/reset/kill/lock functionalities according to corporate policy.	Verify remote functionalities are used when applicable: 1. Identify events requiring remote action 2. Verify appropriate remote functionalities have used accordingly
, 36	Information stored on a mobile device that is no longer accessible may be valuable, either to the user, organization, or					Ensure data can be recovered from a locked device should this be necessary.	Determine how often devices hve been locked during the audit period. For a number of instances, verify data can be recovered.

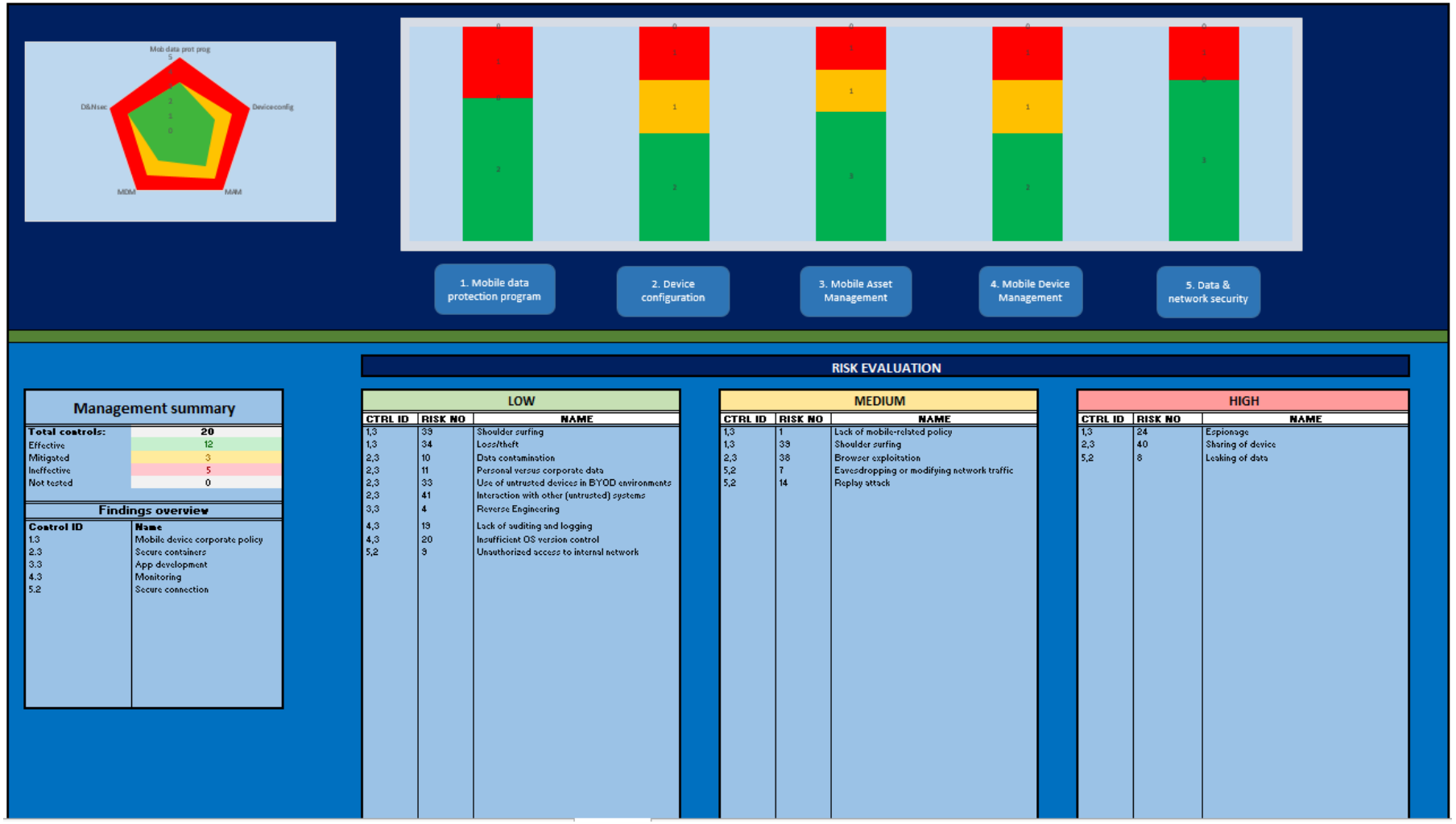
Appendix G.3 Assessment sheet

Assessment sheet

Control Framework				Assessment		
Control Area		ID	Control	Interviewed personnel/ reference material	Evaluation	Notes
1. Mobile data protection program						
1. Mobile data protection program	The mobile data protection program control area contains three controls that together represent all policies and procedures to be set by an organization that relate to ERP mobility.	1.1	Data classification		Ineffective	Test
		1.2	User awareness program		Effective	Test2
		1.3	Mobile device corporate policy		Ineffective	Test3
2. Device configuration						
2. Device configuration	The device configuration control area consists of four controls that all relate to technical configuration of the mobile device before it is commissioned to an employee (pre-configuration) and involves controls that specify how a device should be configured.	2.1	Policy configuration		Effective	
		2.2	Security tools			
		2.3	Secure containers		Effective	
		2.4	User authentication		Ineffective	Test4
3. Mobile Asset Management (MAM)						
3. Mobile Asset Management (MAM)	Mobile asset management (MAM) is about ensuring all assets on the mobile device are secure and managed properly, and consists of five distinct controls that mostly relate to managing apps and maintaining their integrity.	3.1	Selective management		Ineffective	Finding 1
		3.2	White- and blacklists			Finding 2
		3.3	App development		Ineffective	Finding 3
		3.4	App expiration duration		Mitigated	
		3.5	App monitoring		Effective	
4. Mobile Device Management (MDM)						
		4.1	Remote functionalities		Effective	

Appendix G.4 Results overview

Overall assessment



Management summary	
Total controls:	**20**
Effective	12
Mitigated	3
Ineffective	5
Not tested	0

Findings overview	
Control ID	**Name**
1.3	Mobile device corporate policy
2.3	Secure containers
3.3	App development
4.3	Monitoring
5.2	Secure connection

RISK EVALUATION

LOW

CTRL ID	RISK NO	NAME
1,3	39	Shoulder surfing
1,3	34	Loss/theft
2,3	10	Data contamination
2,3	11	Personal versus corporate data
2,3	33	Use of untrusted devices in BYOD environments
2,3	41	Interaction with other (untrusted) systems
3,3	4	Reverse Engineering
4,3	19	Lack of auditing and logging
4,3	20	Insufficient OS version control
5,2	9	Unauthorized access to internal network

MEDIUM

CTRL ID	RISK NO	NAME
1,3	1	Lack of mobile-related policy
1,3	39	Shoulder surfing
2,3	38	Browser exploitation
5,2	7	Eavesdropping or modifying network traffic
5,2	14	Replay attack

HIGH

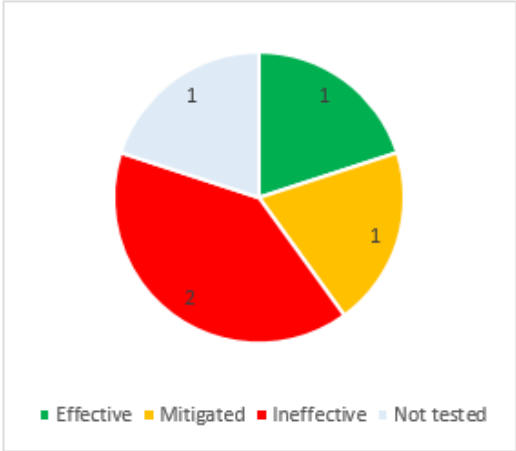
CTRL ID	RISK NO	NAME
1,3	24	Espionage
2,3	40	Sharing of device
5,2	8	Leaking of data

Appendix G.5 Results per area example (MAM)

3. Mobile Asset Management (MAM)

Control area summary

5 controls: 2 effective or mitigated, 2 ineffective, and 1 not tested.



Back to results

Findings overview		
ID	**Control**	**Note**
3.1	Selective management	Finding 1
3.3	App development	Finding 3