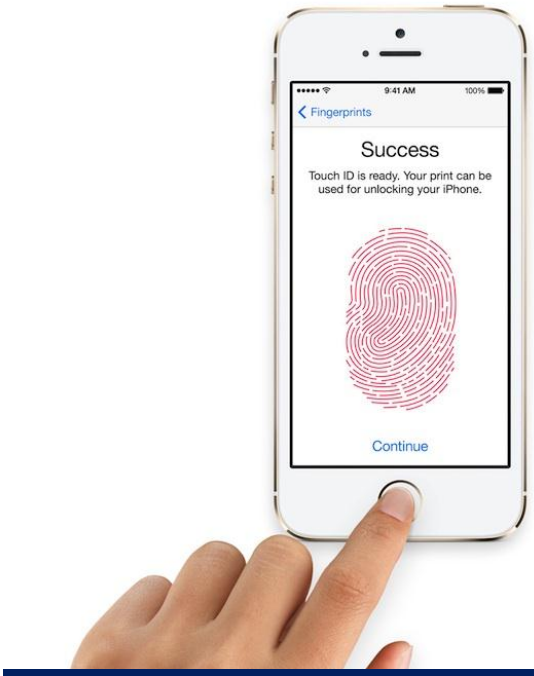
ENTERPRISE MOBILE SECURITY

The development of a Mobile Risk Assessment Method (M-RAM)

"The popularity of mobile solutions seems to outpace the control and governance within enterprise organizations."

Universiteit Utrecht

Deloitte.



Master thesis v1.0 (Final)
November 14, 2013
Joey Janssen (3872092)
Master of Business Informatics
Institute of Information and Computing Sciences, Utrecht University

Supervisors Utrecht University	Dr. M.R. Spruit Dr. R.S. Batenburg
Supervisors Deloitte	Rik Veldhuizen, MSc Rob de Maat, MSc Thomas Bosboom, MSc

Abstract

Mobile solutions seem to outpace the control and governance within enterprise organizations. The acceptance of smartphones and tablets in business has gone at such high pace that organizations are not able to oversee the risks of their mobile usage. Traditional risk assessment methods do not consider mobility despite that enterprise organizations struggle with managing mobile risks. This study aims to fill this gap by introducing a Mobile Risk Assessment Method (M-RAM). The method is based on an extensive systematic literature review and 22 interviews with mobile security managers from external organizations as well as mobile security experts. The final artifact exists out of three components, (1) a risk assessment process that is customized for mobility, (2) involved entities that oppose risks and (3) attention areas that can contain vulnerabilities as well as mitigating controls. Moreover, the study provides an approach to conduct the M-RAM artifact and successfully validates this approach by conducting a case study.

Keywords: enterprise mobility, mobile devices, risk management, mobile security, risk assessment method.

Acknowledgement

This thesis is the final milestone in order to receive a Master degree in Business Informatics from the Utrecht University. I did my very best to make this thesis the master piece of my educational period. This research can be interesting for anyone that concerns the risks of digital technologies and especially the ones that concern risks regarding mobile devices. I hope you will enjoy reading this thesis and will respect my work.

During my research I received amazing support from many persons, in many ways. First I would like to thank Marco Spruit and Ronald Batenburg from the Utrecht University for supervising my thesis project. Secondly, I would like to thank all my colleagues from Deloitte Risk Services and Deloitte Consulting for supporting me content wise, but also process wise. Especially my supervisors Rik Veldhuizen (Consulting), Rob de Maat (Consulting), Robert-Jan Willems (Risk Services) and Thomas Bosboom (Risk Services) really helped me in getting the best results possible. Finally, but very important, I would like to thank my family, friends, and especially my girlfriend for supporting me during this research project.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Research Trigger

The use of mobile solutions within enterprise environments is growing rapidly. “Mobility means more devices, more locations, and more apps”. Information workers that are using more than two devices to do their daily work have risen from 15% in 2011 to 29% in 2012 (Forrester: benchmarking mobile engagement, 2013). The possibilities of mobile devices seem to be endless and replace a lot of conventional desktop solutions. Besides the great advantages of these mobile solutions, there are serious risks that need to be considered, while users are only worried about preserving the convenience on their mobile device (Air-watch, 2013). Arxan (2012) states that 92% of the top 100 paid iOS apps have been hacked compared to 100% of the top 100 paid Android apps.
Identifying and controlling these risks is an immature area and a concern for CIO’s around the world. Information security management is the main focus as mobile solutions are more and more dealing with corporate information using email, mobile ERP applications and corporate portals. The main problem is that enterprise organizations don’t have the means and knowledge to control and govern their mobility usage. Therefore, the demand for a solid approach on identifying and controlling mobile risks within enterprise organizations is growing rapidly.

The consequences of not dealing with the risks that originate from enterprise mobility can be devastating. Leaking sensitive information, violating personnel privacy, violating corporate image, providing access to corporate resources and getting financially robbed through malware exploits are just examples of possible consequences. Financial loss and possible harm to corporations as well as their employees can only be identified when one is able to identify and control the possible threats exposed to the organization.

1.2 Problem Statement

The objective of this thesis project is to develop a method that will help companies in managing the risks that originate from enterprise mobility. The method should (1) enable companies or consulting services to evaluate an existing organization on their current risks regarding mobile security and (2) provide companies or consulting services the means to advise organizations with hands-on solutions to improve their state regarding mobile security.
The problem that is addressed by this thesis project contains of (1) there is no existing method that can be used to assess mobile risks and (2) enterprise organizations are struggling to determine the impact that is created by their mobility usage. The formal and recapitulative problem statement is defined as:

> *“Enterprise organizations are struggling in governing their mobility usage and there is no existing approach that delivers guidance in assessing and managing risks that originate from mobility”*

1.3 Research Question

The main research question is determined so that the problem statement and demand with enterprise organizations is answered.

> *“How can one assess the risks that originate from the usage of enterprise mobility within enterprise organizations?”*

Sub questions

The defined sub questions need to be answered in order to answer the main research question, as each sub question focusses on a specific part of the approach that is needed to assess the risks regarding enterprise mobility within enterprise organizations.

SRQ1: To what extent can traditional risk management processes, standards and models be used for enterprise mobility?

Traditional risk management models are evaluated to determine whether the approaches already address mobile security and/or mobile risk assessments. Furthermore, traditional measures are evaluated on their applicability for mobile usage. SRQ1 also has strong relations with SRQ2, as traditional risk assessment processes or methods are used to determine the needed process steps for a mobile risk assessment.

SRQ2: Which process steps should be taken to assess mobile risks and how should these steps be executed?

This research question needs to be answered in order to be able to define the different steps in the envisioned mobile risk assessment. Each process step should also be executable, as the final approach needs to be operational in order to conduct a case study and use the approach in future projects.

SRQ3: Which entities are involved with enterprise mobility and how are these involved?

In order to design a proper risk assessment approach the entities that are involved with enterprise mobility need to be identified. This question also answers how different entities are related to mobility, how they can initiate risks, but also the risks that an entity has to cope with.

SRQ4: How can mobile vulnerabilities and mitigating controls be identified and categorized?

This research question deals with the most complex part of this research as it needs to answer where the different vulnerabilities with mobility can be found and how the process of identifying these vulnerabilities is executed. Furthermore, a categorization of vulnerabilities and mitigating controls needs to be designed and validated in order to provide the approach structure.

1.4 Scope

Determining the scope in this research is important as this subject can be interpreted in many different ways.
Part of this research is:

- All areas and topics that are related to controlling information security management in the area of mobile devices and solutions
- Information, security and risk management related to controlling and governing mobility
- All trends and external triggers that influence information security management with mobility

Not part of this research is:

- Aspects of mobility governance that are not related to information security management (e.g. device selection, mobility costs, HR policies)
- Reasoning if and when mobile solutions should be used
- Reasoning whether governance is needed with mobile solutions
- Architectural topics on how to create mobile solutions
- Reasoning the technical aspects of information security protocols

- The use of mobile devices as security enablers (using mobile devices to authenticate)

The research domains that are related to this research are:

- Information security management
- IT Risk Management
- Mobile computing

1.5 Definitions

Terms used in this thesis document can sometimes be interpreted in different ways or be unfamiliar for the reader of this document. Furthermore, the gap between the scientific meaning of terms and the business jargon of terms can sometimes result in miscommunications. Therefore, the most important definitions are explained as in how they are used during this research project.

Bring Your Own Device (BYOD): A mobile business model where employees use their personally owned device for business purposes. BYOD is often confused with Choose Your Own Device (CYOD), where employees can choose their own mobile device from a list of approved devices.

Enterprise Mobility: explained 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.

Information risk management: the practice of detecting, evaluating and managing risks that are related to the protection of business critical information.

Mobile Devices: devices as smartphones and tablets that can't be managed like conventional computers and are not within the borders of the corporate building for a substantial amount of time. A more elaborated definition of mobile devices is explained in section 3.2 Mobility.

Mobile Device Management (MDM): Software that enables organizations to remotely control, configure and monitor mobile devices. MDM is mostly used to apply security policies by enforcing security related settings. Extensions of MDM are Mobile Application Management (MAM) and Mobile Content Management (MCM).

Mobile Solutions: Applications that are enabled by mobile devices and mobile software (apps) to support business functions.

1.6 Scientific Relevance

Mobility has been a very emerging umbrella term for various different research projects for the last decade. For example; Mobile Business Intelligence (Verkooij, 2012), Mobile Software Platforms (Anvaari & Jansen, 2010) and Smartphone apps (Xu et. Al, 2011). These scientific research projects often have close relations to business environments were mobility solutions in for example banking and medical industry have been adopted very fast over the last decade (Wu .I et. Al, 2011 and Lin, 2011). Despite the various research projects on mobile technologies and solutions, there seem to be very little research conducted in the field of mobile risk assessments in the highest level of enterprise organizations. Mobile information, security and risk management are fields that are already more active within research. Though, most of the research in this field is on device level.

The scientific relevance of this project is the development of a theoretical framework that will provide insight and guidelines to all aspects regarding mobile risks. Furthermore, the combination of extensive literature research and broad field research with Deloitte consultants will provide the ability to validate this theoretical framework and determine all activity in the field of mobility.

Social-business relevance

Controlling and governing mobility is an immature area and a concern for CIO's around the world. The lack of a well-substantiated framework based on scientific research and business experience results in the inability to control and govern mobility for corporate organizations.

Furthermore, organizations are not always aware of the risks and impact that are taken with mobile solutions. "The popularity of mobile solution seems to outpace the control and governance within corporate organizations" describes the social problem and relevance for corporate organizations. The aim of this research is to bridge the gap between using & applying mobile solutions and being able to still control and govern the underlying risks and impact to the organization.

1.7 End Deliverable

This research aims to develop an artifact in the form of a method. The artifact should be in the form of a method as it aims to provide an executable process containing an approach and guidelines to properly use the artifact. The artifact should be used by organizations, researchers or consultants to identify the risks that originate from enterprise mobility and how an organization deals with these risks. The artifact is named the M-RAM (Mobile Risk Assessment Method) as this name best covers the potential of the artifact. Based on the method components that are explained in section 4 , the construction of the M-RAM artifact will be explained in section 5 Artifact Components.

2 Methodology

This chapter elaborates on the explained research approach in the introduction. Section 1.6 provides a practical view on the steps that will be taken to complete this research. This chapter concentrates on the theoretical and scientific justified methodologies that are used to conduct this research.

2.1 Design Science Research

In the research field of information systems (IS) two main research paradigms are identified, namely behavioral science and design science (Hevner et al., 2004). Behavioral science is explained as the research that develops, explains and predicts the behavior of organizations regarding the development, usage and management of information systems. The second research paradigm, design science focusses on the development of new artifacts that contribute to the body of knowledge in the field of IS (Simon, 1996). Design science is used for solving practical problems in the field of IS, by creating innovative artifacts (Hevner et al., 2004).

As the aim of this research is to introduce an innovative method that assesses the state of mobile security of an organization, design science is very well suitable for this research. This is because the mobile security assessment method will be a new and innovative artifact that contributes to science, which is the underlying goal of design science. To ensure the quality of design research, Hevner, March, Park and Ram (2004) provide seven guidelines that ensure the quality of the created artifact. Each principle is respected during this research and is explained and related to the research below:

1. **Design an artifact** - *"Design science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation"* (Hevner et al., 2004). This research produces a method containing a high level framework. The method can be used to assess organizations on their mobile security state.
2. **Problem relevance** - *"The objective of design science research is to develop technology-based solutions to important and relevant business problems"* (Hevner et al., 2004). This research combines traditional security and governance technologies as well as state of the art mobile management technologies to assess the risks that are involved when using mobility for business objectives.
3. **Design evaluation** - *"The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods"* (Hevner et al., 2004). The evaluation of the method artifact is done through a vast amount of expert interviews containing mobile security consultants, mobile security product experts and mobile security managers from different renowned organizations as described in section 4.1 . Furthermore in section 7.1 Case a case study is performed and evaluated to validate the efficacy and utility of the artifact.
4. **Research contributions** - *"Effective design science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies"* (Hevner et al., 2004). The scientific and social-business contribution of this research can be found in 1.6 Scientific Relevance.
5. **Research rigor** - *"Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact"* (Hevner et al., 2004). The construction of the artifact is done through rigorous evaluation methods on existing methods and an iterative process of evaluating the method (high level framework) with domain experts.
6. **Design as a search process** - *"The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment"* (Hevner et al., 2004). The obtained means from scientific literature and domain experts are used with respect to the problem environment.
7. **Communication of Research** - *"Design science research must be presented effectively both to technology-oriented as well as management-oriented audiences"* (Hevner et al., 2004).

This thesis can be read and used by audiences that are scientific, technology as well as business oriented. This is achieved by respecting the scientific writing style as well as addressing the practical problem from a business perspective.

Behavioral science is only suitable and used for the rationale validation of this research, as it used to explain how organizations are dealing with mobile security.

2.2 Research Process

This section describes a high level approach that is used for design research as well as a detailed research process that defines 12 steps that are taken to create and validate the intended artifact.

Vaishnavi and Kuechler (2007) provide high level process steps for Design Science Research in Information Systems (DSRIS) projects. The design research cycle containing these process steps is based on earlier work from Vaishanvi and Kuechler (2004). The five process steps: Awareness of problem, suggestion, development, evaluation and conclusion are divided in an abduction part and a deduction part. The first two steps represent the abduction formalism and the last three steps the deduction formalism. The first step, creating awareness on the problem is done by creating and communicating the long proposal, which includes the problem statement and relevance of this research. In the second step, suggestion, a conceptual high-level framework is created to envision the final deliverable method. This step contains several iterating changes that are triggered by expert insights or literature statements. The third step is the development step, where the high level conceptual framework is transformed to the detailed method. This step also incorporates the validation of each part of the method, internally as well externally. The evaluation step is an important step as the method is evaluated on its suitability by performing a case study. Furthermore, the evaluation step concludes whether the research questions are answered in a proper way. The last step concludes the communication and conclusion of the research.

The substantive process to this research is also specified by the use of detailed steps. Each step is reflected to the problem solving process derived from Mitroff et al. (1974). In Figure 1: Method visualization the steps are modeled to the two axes time (current situation / improved situation) and environment (model world / real world) introduced by Mitroff et al. (1974). The figure provides a quick overview of the steps that need to be taken during this research; each step will be elaborated in this chapter. The process flow starts with step 0 (green), representing the research trigger created by the market demand and problem situation.

1. Systematic literature review on information security management and governance in mobility as well as conventional situations. The Systematic Literature Review (SLR) will be focused on publications from the last 5 years, as mobility is still new to the field of information security management and governance. The main SLR key words will be: mobility, IT governance, information management, security management, BYOD, mobile device management, risk management, demand management and availability management.

2. Evaluating existing governance and security documents on their suitability for current mobile environments. This step contains the evaluation of existing models as COBIT, NIST and several ISO/IEC models on their suitability for and attention on mobility. The findings from the SLR in step 1 will be used to evaluate the models on their mobile suitability.

3. Determining existing threats, vulnerabilities, risks and mitigating actions regarding mobile security & risk management. Based on step 1, exploratory semi-structured interviews with consultants and the latest reports on mobile risks and security.

4. Identify research gap, demand and shortcomings regarding mobile risk assessments with Deloitte consultants by using semi-structured interviews.

5. Conduct interviews with mobile security managers and mobile security experts to identify how organizations think about mobility, how they are dealing with mobile security and how their mobile risk management is organized.

6. Determining mobile gaps and shortcomings in existing risk assessment methods.

7. Determine risk assessment process including threats, vulnerabilities, risks and mitigating actions regarding mobility.

8. Determine the entities that are involved with mobile security based on step 1 till 5.

9. Determine mobile security attention areas based on step 1 till 5.

10. Create the high-level artifact using the output of step 7, 8 and 9.

11. Specify practical approach and guidelines for using the designed method.

12. Verification of theoretical method and practical approach with Deloitte consultants and external mobile security experts. Furthermore one or more case studies with independent Deloitte clients will be conducted, to verify the framework.

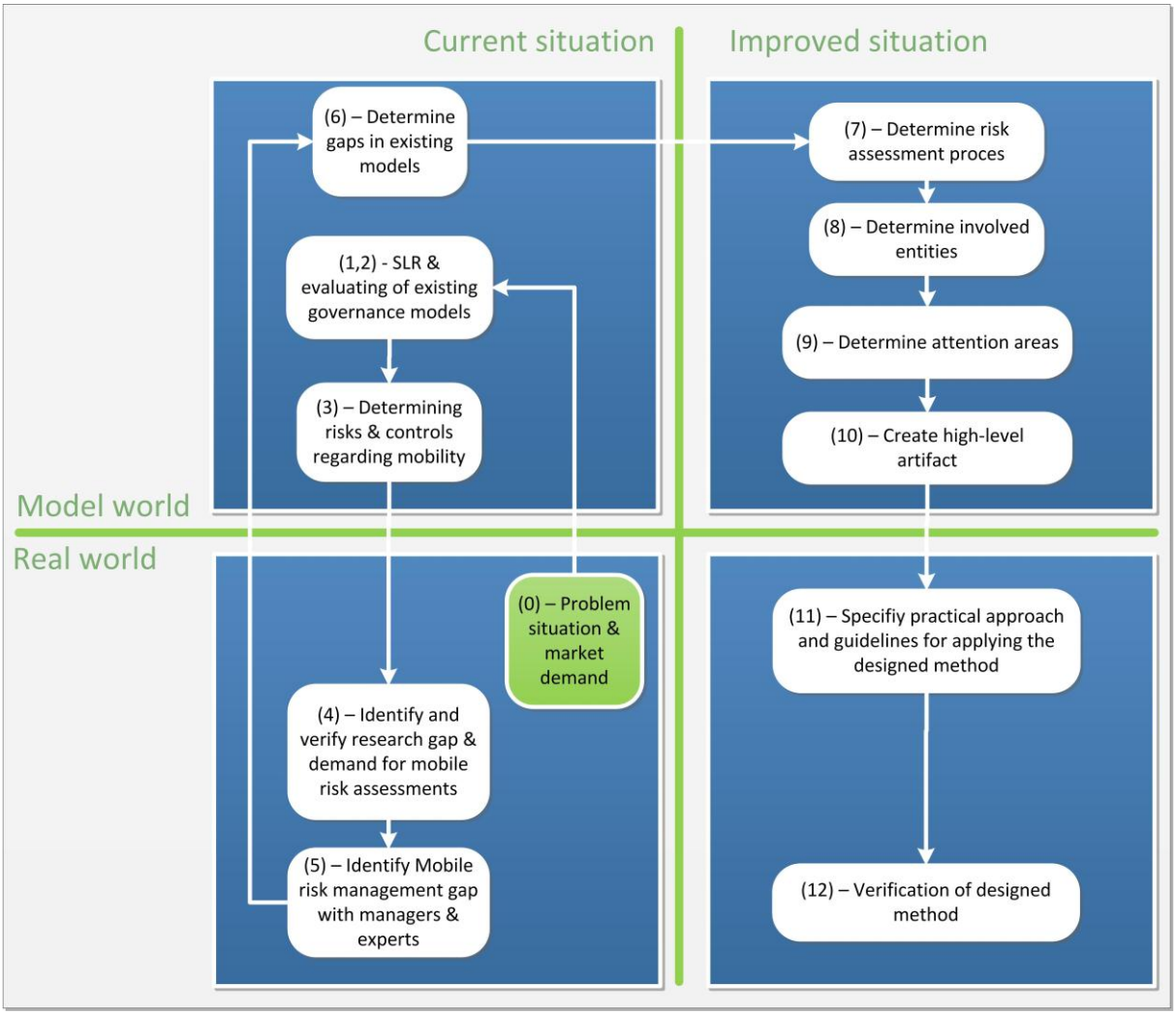


Figure 1: Method visualization

2.3 Systematic Literature Review

One of the goals of a SLR is to position the research in the existing body of knowledge regarding the thesis topic (Hart, 2011). Furthermore, it is key to have a good understanding of common techniques, terminology and proven concepts to understand the field of research and be able to conduct proper research (Hart, 2011). The SLR is also used to identify areas that still need to be researched and areas that are already been broadly examined. (Webster & Watson, 2002). This prevents that this research will present biased or already presented results. The existing models, frameworks and other artifacts processed in the SLR are used as a basis for the envisioned artifact as these provide a fundamental basis (Hevener, 2004).

Conducting a proper SLR requires the use of a rigorous method that suits the IS research field. Duff (1996) provides a method that is especially designed to conduct literature reviews on a high and more abstract level like information sciences. As the mobile security field is still very immature, this method is very useful. The method exists of five stages that are visualized in Figure 2: SLR method by Duff (1996) and elaborated below.

Figure 2: SLR method by Duff (1996)

Create set of search terms – the first step is to create a set of search terms that is broad enough to result in a sufficient amount of scientific articles. As the research field is still very immature, the scope of search terms should be very elaborate. Furthermore, mobile (security) technology has changed very rapidly over the last few years, which means that publications older than three years are already obsolete.

Formulate search terms – this step is used to translate the search terms in usable strings. For the used search machines the search terms need to be between brackets (“”). No other actions are required to conclude the search action.

Estimate search parameters – Duff (1996) states that there are four parameters that need to be defined in order to estimate the relevance of any result. If a result doesn’t meet one of the parameters it is likely that it is not relevant to this research. However, it does not mean that it’s already removed from the possible useful results (Duff, 1996). The first parameter, spatial, is used to define the geographical area of the research. This research is not especially bound to a geographical area but there is a geographical difference that should be taken into account. European countries are lacking behind on mobile security innovations compared the USA (Cisco, 2012), this means that an European article from a certain year is already outdated, while a paper from the USA is still recent enough. This acknowledgement is already related to the second parameter, which is temporal. The temporal parameter states that used articles should always be recent with respect to the body of knowledge of the specific field.
With this research a short time span of three years is used as the subject is very sensitive to be outdated. So each search action is performed on articles that are published after 2009. A time frame of the last three years is chosen because this subject has only been active since the last few years and earlier publications regarding more traditional topics as information security would not be relevant anymore, due to outdated technologies.
The third parameter, disciplinary defines the different research fields that are related to the research. These research areas are already defined in 1.4 Scope.
The last parameter is focused on the formal acceptation of sources. The SLR is focused on scientific respected sources (Conference proceedings, academic journal articles, dissertations and books). However, since the research topic is very topical in the corporate business environment, there are a lot of publications that can be defined as so called ‘grey literature’ (Petticrew, Roberts, & MyiLibrary, 2006). Research organizations as Forrester, Gartner and IDC are examples of these sources. Grey literature will not be processed in the SLR but will be used to backup statements of expert interviews or scientific sources.

Search information sources – The meta-search engine Google Scholar is used as the primary search engine for this research project. A meta-search engine is an engine that interfaces with different existing conventional search engines and combines the results, ordered on relevance (Dreilinger & Howe, 1997). Besides Google Scholar, two highly related search engines (IEEE Explore and ACM) are used to keep the SLR rigorous.

Record and evaluate references – The results of the SLR are recorded in Figure 4: SLR results in section 3.1 SLR Results. For each search term the number of results per search engine is provided. After processing the search queries the results are filtered based on their title. The second step

involved a check on the availability of the articles. Most of the articles were directly available by a PDF download or referral to a webpage. Articles that were not directly available, but very interesting to the research are obtained by contacting the author or paying an acceptable fee. The remained papers are then assessed by reading the abstract of the paper. The abstracts and article outlines are evaluated on relevance to the research, status of the author, citations and recentness of the topic. The articles that satisfy the stated criteria are read, annotated and then processed and linked to topic related nodes using NVivo 10. The topic related nodes are used to divide all references over the different subjects so that found information can easily be used during the research. Figure 3 provides an overview of the topic segmentation.

Nodes

Name	Sources	References
Background	20	63
BYOD	9	23
Demand & Usage	8	20
Framework	2	2
IS Governance models	1	10
MDM	13	33
Mitigating Actions	3	3
Data (network access)	10	24
Device (apps)	21	50
Governance (privacy & policies)	14	51
Process	8	11
User	6	8
Risk assesment	5	11
Survey tips	1	1
Threats	16	40
Vulnerabilities	3	3
Data (network access)	3	4
Device (apps)	5	10
Governance (privacy & policies)	2	2
Process	0	0
User	8	18

Figure 3: NVivo nodes segmentation

2.4 Expert Interviews

The knowledge of experts is one of the main sources for this research as they are working in the constantly changing environment of mobile security. A qualitative approach is chosen over a quantitative approach as the field is not yet explored enough to be able to set up a theoretical grounded survey or other quantitative approach (Jacobsen & Hellstorm, 2002). There are two different types of actors in the field of mobile security that need to be considered regarding this research. The first actor is the person that is responsible for mobile security within a corporate organization. The second actor is the person that is a specialist on mobile security and is in the role of advising other organizations on how to deal with mobile security.
For both actors a different semi-structured interview protocol is designed to be able to guide the interview without hindering the ability to capture valuable information (Barriball & While, 1994). The interview protocols can be found in Appendix A – Interview protocols.

Practical interview execution

The interviews are mostly conducted at the office of the interviewed manager/expert with an exception of experts that were not situated in the Netherlands (A videoconference was used to conduct the interview). All interviews had a duration of approximately one hour, as agreed by the interviewee. After receiving permission, all interviews were recorded using a smartphone. Each interview started with an introduction of the interviewee and an introduction of the research project, discussing the goal, stakeholders and research problem. The substantive part of the interview was divided in the following sections, demand & usage, threats, vulnerabilities, risk & impact, mitigating controls and risk evaluation. After finishing the interview, the results were transcribed to text files.

2.5 Case Study

The M-RAM artifact is based on theoretical knowledge and constructed using a design science methodology. A case study is a proper method to validate the construction of the M-RAM artifact (Vaishnavi & Kuechler, 2007). The method focuses on organizational behavior, business events and political forces. These properties can best be validated in a real life environment as these properties cannot be simulated in a non real life environment (Yin, 2009). Gorman & Carlson (1989) explain the difference between a confirmatory case study strategy and dis confirmatory case study strategy. The confirmatory strategy tries to confirm the constructed artifact by comparing results from multiple cases, where the disconfirmatory strategy uses one case study and only identifies when a certain part of the case study cannot be executed. This study applies a disconfirmatory strategy as there is only time to conduct one case study.

In order to conduct the envisioned case study, a practical method of the theoretical constructed M-RAM artifact needs to be defined. Section 6.2 Method explains a possible method interpretation of the theoretical M-RAM approach. This method is used to perform the case study and will later be evaluated on its applicability in practice. In order to achieve a rigorous disconfirmation with a single case study, it is essential to select a case that is representative for comparable situations (Cavaye, 1996). Furthermore, a set of selection criteria is determined to ensure the case provides; (1) a high probability of validating the theoretical artifact, (2) the right maturity level of enterprise mobility, (3) a cooperative organization and (4) challenging business process that pull the most of constructed artifact. The following criteria were set to select a case study:

- The case study organization is willing to participate and cooperate within the case study and values the output of the M-RAM assessment.
- The case study organization uses multiple mobile devices for multiple purposes, supporting primary as well as supportive business processes.
- The case study organization has to cope with sensitive information assets on mobile devices that challenge the risks regarding enterprise mobility.

After conducting the case study, the study will be evaluated and the M-RAM artifact will be adapted to the findings in the case study.

3 Theoretical Background

This chapter provides a good understanding of the research areas and their respected terminology that are related to this thesis research. The first section, 3.1 SLR Results provides the output of the SLR that is conducted at the beginning of this research. The output of the SLR is used to provide the theory of this chapter as well as all literature that is gathered after the SLR. Section 3.2 Mobility explains the general understanding of mobility, mobile apps, mobile devices and all other activities that are part of mobility. Section 3.3 Mobile Security explains traditional security standards, mobile security standards and their relation to each other. Section 3.4 IT Risk Management provides an overview of traditional IT risk assessment models and their applicability for mobile risk assessments. The last section 3.5 Research Gap explains the research gap between existing risk assessment methods, security measures and the knowledge to govern mobile information and security and a Mobile Risk Assessment Method (M-RAM).

3.1 SLR Results

Figure 4: SLR results provides an overview of the SLR conducted, following the approach as described in 2.3 Systematic Literature Review. The final list of search terms is:

- "Mobile Security"
- "Information Security"
- "Mobile Device"
- "IT Governance"
- "Mobile computing"
- "Mobile risk"
- "Mobile governance"

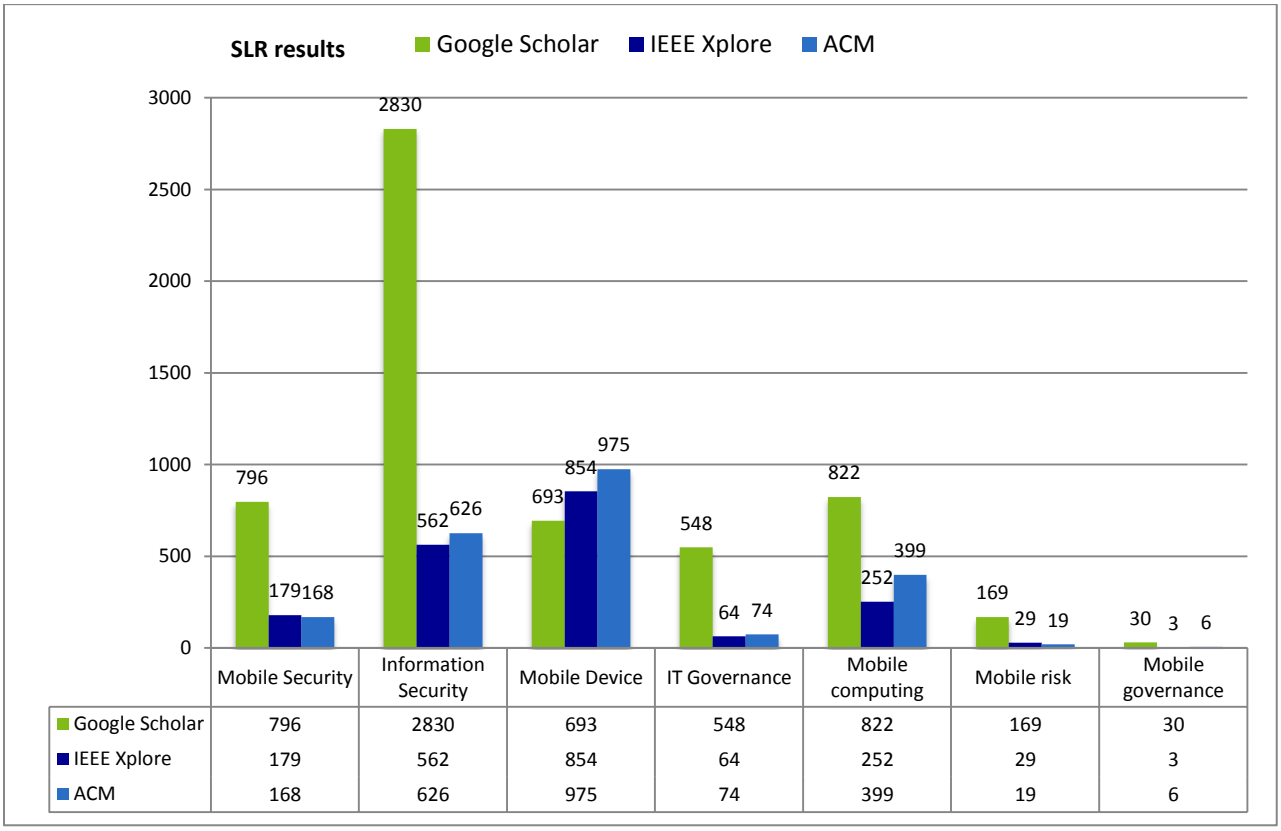


Figure 4: SLR results

The earlier mentioned term ‘mobility’ is not used in the keyword search queries as authors mostly refer to the term ‘mobile’. Mobility can still be used as a valid term when summarizing mobile activities.

3.2 Mobility

The beginning of the smartphone era can be seen as compared with the beginning of a new millennium. Since then, numerous new “smart” devices like BlackBerries, iPhones and Android-based phones have been introduced that revolutionized the market (Becher et. al, 2011). Mobility is a collective noun that represents all activities that are part of this mobile revolution. These activities include the usage and management of mobile devices, the practice of connecting mobile devices with the Internet or information resources and the usage of mobile applications (apps).

Mobile device

Mobile device, smartphone and tablet have become common accepted terms, but the classification of devices is still often discussed. Some people even suggest that laptops are also considered mobile devices. Derballa & Pousttchi (2004) state that laptops are not truly mobile but should be identified as portable devices. Moreover, Rasmussen, Chen, and Bansal (2009) state that “Mobile devices, given their fundamental purpose, should be small and portable”. Schwartz (2006) states that “Laptops can be moved easily, but they are usually not used during that process”. This research follows these statements and does not consider a laptop as a mobile device. However, as more and more Hybrid devices like Phablets (Forbes, 2012) and Hybrid laptops (PCMag, 2013) occur, the line between mobile devices and laptops is getting blurred. For this study Phablets are considered as mobile devices where Hybrid laptops are evaluated on their purpose and features to decide whether they are considered as mobile devices. The Windows Surface tablets are defining the line between a tablet (mobile device) and a laptop (not considered as a mobile device) the best way. The Surface RT is seen as a mobile device where the Surface Pro is seen as a laptop. The distinctive property for this consideration is based on the operating system of the devices. The Surface RT has no full-fledged Windows 8 operating system as it is not possible to run Windows software that is not available via the App store, where the Surface Pro has the ability to run traditional Windows software (Microsoft, 2013). From a security perspective another very clear distinction can be made. In contrast to the Surface Pro device, the Surface RT device can’t be managed via traditional security measures as Group Policy, enhanced data protection using BitLocker technology, compatibility with third party security management and monitoring applications. Furthermore, less punctual properties as portability, corporate domain connection and connectivity define the difference between the two devices and thus a tablet and a laptop (Microsoft, 2013). NIST (2012) has established a baseline of software and hardware characteristics to define a “mobile device”. These characteristics are listed below and are also used as a baseline for this study.

- *A small form factor*
- *At least one wireless network interface for Internet access (data communications). This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with Internet connectivity.*
- *Local built-in (non-removable) data storage*
- *An operating system that is not a full-fledged desktop or laptop operating system*
- *Applications available through multiple methods (provided with the operating system, accessed through web browser, acquired and installed from third parties)*
- *Built-in features to synchronize local data with a remote location (desktop or laptop computer, organization servers, telecommunications provider servers, other third party servers, etc.)*
- *One or more wireless personal area network interfaces, such as Bluetooth or near-field communications*
- *One or more wireless network interfaces for voice communications, such as cellular or Global Positioning System (GPS), which enables location services*

- *One or more digital cameras*
- *One or more microphones*

Future devices will change the definition of a mobile device as hardware and software specifications are changing rapidly and becoming more and more interchangeable. In section 4.1 mobile security managers will provide their opinion on what they consider mobile devices and how this will change in the near feature.

Mobile App

The applications that are running on mobile devices are called apps, an abbreviation of applications. Lerotic states that from 2010 and onwards, 'app' is used to imply applications for mobile applications (Lerotic, 2012). Mobile devices are of the shelf delivered with standard apps to provide the basic functionality like mailing, browsing and an agenda.

In 2008 Apple was the first to announce that third party apps were allowed to run on their mobile devices (Godwin-Jones, 2011). Apple provided an SDK (Software Development Kit) to develop the mobile applications and also introduced an environment, the Appstore where apps could be sold and downloaded. Bloemendal (2012) defines an app store as follows: *"An app store is an online curated marketplace serving one or more software ecosystems that allows software developers to sell and distribute their products to users of a software platform"*. With "an online curated marketplace" Bloemendal (2012) distinguishes the normal brick and mortar stores to an online variant; curated means that there is one party that selects and monitors the goods (apps) that are being sold.

Mobile apps can be used for different purposes, work as well as private related. Hyrynsalmi et al. (2012) define different categories that are used by appstore vendors to help users find the app they are looking for. Apps are also distinguished by their business model. There are free apps, payed apps, but also more complicated business models such as in app purchasing, advertisements and monthly subscriptions (Xia, Rost & Holmquist, 2010). Businesses and mobile app developers nowadays often choose to develop their apps for multiple platforms (E.g. Apple appstore, Google marketplace), this behavior is also referred as multi-homing between appstore ecosystems (Idu, van de Zande & Jansen, 2011). As the appstore vendor controls the purchasing and downloading of apps, businesses have very little control on the applications that are downloaded and used by their employees. Therefore enterprise appstores are introduced that allow an enterprise to control, monitor and distribute third party and self-developed mobile apps (Rouse, 2012). The security measures that are taken to secure mobile apps are explained in 3.3 Mobile Security.

Mobile Business

The field of mobile business is very broad as almost all traditional IT and business related topics are transformed to a mobile version. The definition mobile business is therefore very broad. Tarasewich, Nickerson and Warkentin (2002) define mobile business as "all activities related to a (potential) commercial transaction through communications networks that interface with mobile devices". Another definition is provided by Paavilainen (2002) which states that mobile business is: "The exchange of goods, services, and information using mobile technology". Derived from the International Conference on Mobile Business (ICMB) an overview of mobile business areas is explained in Table 1: Mobile Business Each area is elaborated with one or more examples. The derived areas can be categorized in two main professional fields, namely 'Mobile app development' and 'Enterprise Mobility'. Mobile app development is focused on the practice of developing apps for consumers or business partners. This research only deals with the field of Enterprise Mobility, which focuses on the internal use of mobile devices within enterprise organizations.

Mobile Business Area (ICMB)	Example Services	Derived categorization
B2C services and applications	Mobile parking, Mobile marketing, Mobile advertising	Mobile app development
B2B services and applications	Enterprise applications, integrated business processes	Mobile app development
Public services	M-health, Mobile Government	Mobile app development
Legal, societal and political aspects	**Privacy and trust, Consumer protection, Regulatory issues**	Enterprise Mobility
Mobile Technologies	Network standards, RFID, NFC	Enterprise Mobility
Platforms and Infrastructure	Sensor networks, **Mobile security**	Enterprise Mobility

Table 1: Mobile Business categorization

Schadler & McCarthy (2012) states that enterprises need to align the demand of the mobile apps that business owners want to build and the requirements that are needed to service the desired apps. Furthermore, Schadler & McCarthy (2012) suggests that a new role called the Chief Mobility Officer (CMO) needs to be introduced in order to realize this alignment.

Bring Your Own Device (BYOD)

When discussing enterprise mobility, Bring Your Own Device (BYOD) is a term often used in science as well as the business domain of enterprise mobility. Morrow (2012) defines BYOD as the practice where *"employees, business partners and customers are increasingly accessing information using a web browser on a device not owned or managed by the organization."* Trustwave (2013) defines BYOD as an employee driven mobility initiative where personally owned devices are used for work related activities. Harris, Patten & Regan (2013) state that BYOD means that employees use their own devices for personally as well as business related tasks at the same time. BYOD has evolved because employees resisted complying with corporate security policies that denied access to personal applications, mail and especially social media (Trustwave, 2013).

Recent studies show that not only personally owned devices are brought and used at work but also apps, content, services and other variations are used. Shim (2013) explains the differences between Bring Your Own Services (BYOS), Bring Your Own Application (BYOA) and Bring Your Own Content (BYOC). Morrow (2013) defines this diversification by stating that the 'D' in BYOD can be seen as any personal internet connected device using any kind of application or service connected to a corporate environment. BYOD is also often related to the 'consumerization' of information technology, which is explained as the use of consumer devices for corporate tasks (Harris, 2012). Niehaves, öffer, & Ortbach (2012) define 'IT consumerization' as using privately-owned IT resources for business purposes. They also state that 'IT consumerization' redefines the relationship between employees and the IT organization.

BYOD can bring great productivity improvements for businesses but also brings an enormous risk assessment problem to businesses (Symantec, 2012). *"While most IT professionals agree mobile devices pose major security risks, there is a major lack of mobile device security awareness and training programs in organizations."* (Harris, Patten & Regan, 2013). The problem with BYOD is that employees want to use whatever device, app or data they want, which makes it very hard to manage BYOD. The management of BYOD will be further discussed in section 3.3 Mobile Security.

3.3 Mobile Security

Mobile devices are more and more enabled to extensive functionality and used to store sensitive personal or business information. This occurrence makes mobile devices an interesting target for hackers or other malicious actors (Oberheide, 2010). The importance of mobile security is no

discussion, but the way mobile security should be enabled is still often hard to define. Leavitt (2011) states that after years of warnings about mobile security threats are becoming reality in the form of viruses, malicious applications, spyware and phishing applications. A recent report from Lookout (2012) concludes that mobile threats evolve together with the evolution of mobile devices. Mobile malware is already a profitable business a great threat in certain parts of the world. This section explains existing mobile attack vectors and the taken remedies to cope with these attacks.

Attack vectors

"As more and more sensitive data such as login credentials are stored on mobile devices, attackers may still wish to target them for harvesting data (Oberheide, 2010)." Different attack vectors can be used to harm mobile users and often gain the desired information. Becher et Al. (2011) classifies the different high level methods that a mobile attacker can have. These methods can be used to identify possible threats for organizations. The first method is 'Eavesdropping', where someone intentionally or unintentionally follows a conversation of someone and depicts (confidential) information from the conversation. The second method is to disrupt the usage of a device and can be achieved using an availability attack. Privacy attacks are used to gain personal information about the user of the mobile device, which is classified as the third method. The last method is an impersonation attack where the attacker impersonates a device to gain access to other resources such as corporate information systems.

Lookout (2012) states that mobile attack vectors are diversifying and changing rapidly. They also state that the geographic location influences the sort of attack users have to deal with. For example malware attacks on Android are much more likely in Russia, Ukraine and China than in other countries (Lookout, 2012). The report shows different successfully executed mobile malware attack vectors. The most common malware attack vector is 'Toll fraud' which bills unsuspected victims with premium SMS services. Dagon, Martin and Starner (2004) state that mobile information attacks can be classified in two categories, namely transient information and static information. Transient information is defined as all meta-information that is telling something about the device (I.e. battery usage, memory addresses and location data). Static information is explained as the information that is stored on the device or sent by the device (I.e. contact information, corporate information and notes). Furthermore, two different Denial of Service (DoS) attacks are categorized for mobility. The first category attempts to flood the device so it can't handle the requested actions, where the second category tries to drain the battery so the device can't be used anymore (Dagon et Al., 2004). Rootkits, malware that stealthily modifies operating systems to achieve their malicious goal have been a problem for traditional operating systems. Bickford et Al. (2010) shows that mobile devices are just as vulnerable for rootkits as traditional computers are. However, the unique interfaces of mobile devices make the consequences of rootkits even more impairing (Bickford et Al., 2010).

Vulnerabilities

The definition of 'vulnerability' is often confused or interchanged with the definition of 'exploit' or 'threat'. Within the context of this research, a vulnerability is a weak spot that possibly enables (malicious) parties to exploit (make use of) the weak spot. When the vulnerability can be exploited it becomes a threat to the organization or targeted party. A survey study by Tenable Network Security (2012) concludes that 70% of the respondents find that mobile device vulnerability management is one of the top security priorities. Also, almost all respondents say that mobile devices are a great security threat to their organization. On the other hand, 68% states that they don't know how to properly identify mobile vulnerabilities and that they don't have proper controls to mitigate these threats (Tenable Network Security, 2012). Organizations that do know how to identify and manage mobile vulnerabilities are only able to identify common and already known vulnerabilities. Codenomicon (2010) states that the main security challenge lies in the unknown vulnerabilities, that are constantly changing as devices, mobile operating systems and apps are releasing updates on a daily basis.

The most common discussed vulnerabilities are software vulnerabilities, weak spots that possibly can be exploited in a mobile operating system or a mobile app. However, in the context of enterprise mobility, vulnerabilities can also be identified on an organizational or individual level. Morrow (2012) explains how users can become vulnerable by not being aware of the risks that they are creating by for example storing corporate attachment on a local SD card that can be exploited easily. Becher et. Al (2011) states that 'user layer attacks' are an important class of vulnerabilities. Device hardware and network connection vulnerabilities also need to be taken into account with mobility as devices are often lost or stolen and devices make connections with lots of different insecure networks (Becher et. Al, 2011). Vulnerabilities can also be classified on a different level. Sybase (2013) defines the following four vulnerability areas within the mobile business; (1) Lost or stolen devices, (2) unauthorized data access, (3) Mixing up personal usage with enterprise usage and (4) not being able to enforce defined policies. Despite the fact that Sybase (2013) uses 'vulnerability' and 'risks' interchangeably, the four areas can be related to earlier described vulnerability layers. The first two areas can be linked to device vulnerabilities, the third to user layer vulnerabilities and the fourth area can be explained as a vulnerability area on organizational level.

Without explaining vulnerabilities for specific devices, OS versions or mobile apps a general mobile vulnerability needs to be discussed. Jailbreaking or rooting of a mobile device makes the device extremely vulnerable for exploiting exposed vulnerabilities on operating system level. Miller (2011) provides a clear explanation on the technological consequences of jailbreaking: *"Jailbreaking disables code signing on iPhones to run apps not from the App Store. This breaks almost all the protections iOS offers. First, it disables code signing, which opens the platform up to malware. In addition, many of the added non-signed applications run at the root level without a sandbox. The jailbreaking patches also somewhat disable data execution prevention by allowing writable and executable memory, which isn't normally in iOS (Miller, 2011)".* Jailbreaking or rooting is an operating system vulnerability that is initiated by the user itself. The reason why users are jailbreaking / rooting their device is to run non-signed and thus non approved apps on their device.

Device security

The security of mobile devices can be compared to the security of traditional computers but has also very distinctive properties compared to traditional computers. Becher et. Al (2011) provides an overview (Figure 5) of security related properties that are different with mobile devices compared to traditional devices. The creation of cost is two factor, mobile devices are creating cost by the different cellular services they use but can also make use of mobile banking payment services. The network environment of mobile devices is different in three areas. First the connection of mobile devices is very different as the connection is made using a network operator's SIM-card. Also the firmware of mobile devices is often pushed over the network and installed wirelessly. The third difference is related to the management of mobile devices. Different entities (I.e. Enterprise organization, network operator and device manufacturer) are able to manage a mobile device and for instance wipe the device remotely.

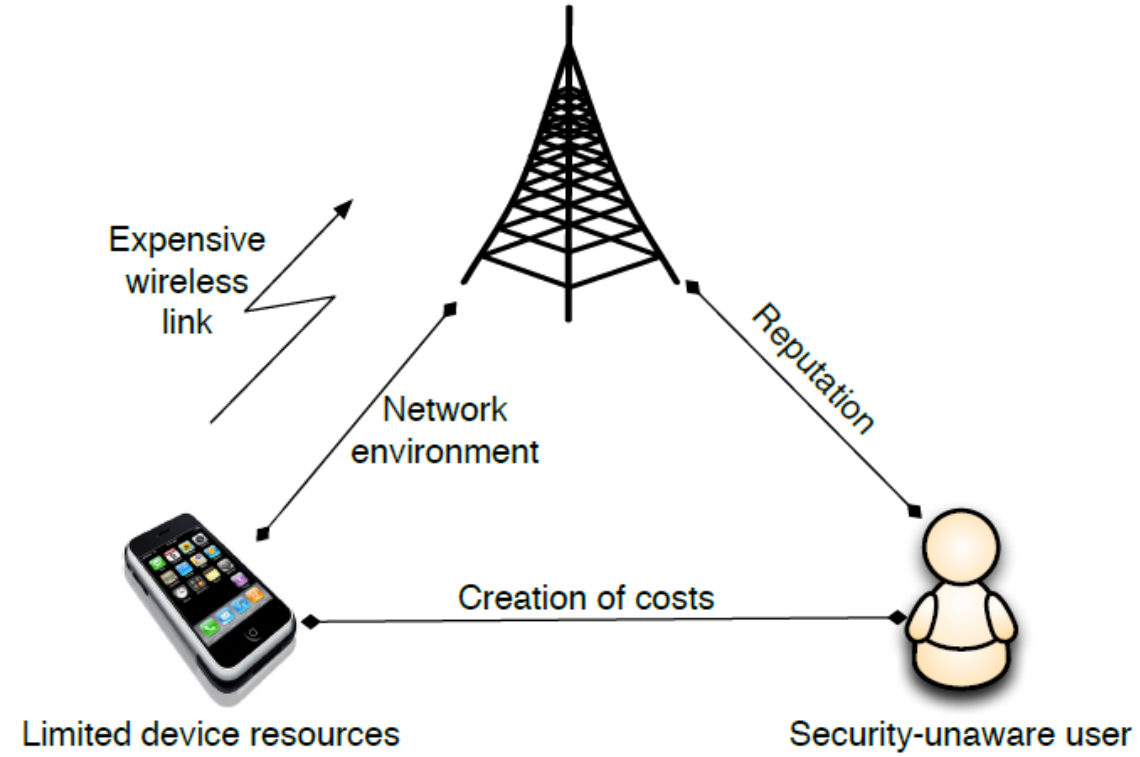


Figure 5: Specific security properties for mobile devices (Becher et. al, 2011)

The limited resources of a mobile device also change the security possibilities. As mobile devices are becoming more and more advanced the limitation of computing resources becomes obsolete, the limited battery however is still a limitation for advanced security measures.

Google's Android and Apple's iOS are responsible for 92.3% of all mobile devices' operating systems and can be seen as the largest and most mature mobile operating systems (IDC, 2013). As a theoretical basis for device security the standard security controls of both Android and iOS are evaluated as they are available in the latest OS versions in July, 2013. Miller (2011) explains the security measures of both Android and iOS. The measures are focused on the two most common attacks, mobile malware and exploiting OS vulnerabilities, which are used to run any kind of malicious code that attackers want to run on a mobile device. The malware controls of iOS are very extensive. First, iOS is using a closed appstore ecosystem by reviewing and signing all applications with Apple's private encryption key (Jansen & Bloemendal, 2013). If any app manages to get around Apple's reviewing process, Apple deletes the app from the Appstore and remotely wipes it from devices. Furthermore, apps are directly sandboxed when installed on the device. Sandboxing means that the app cannot access or be accessed by any other app without the user's permission (Seriot, 2010). The malware controls of Android are far less extensive compared to iOS. There is no app review process in place, which means that any app can be uploaded to the Android market. Developers can also sign their own applications, which means that apps can be installed from any resource and thus not only from the Android ecosystem. Google uses crowdsourcing to gain information about the quality of an app. When an app has lots of bad reviews and malicious behavior is detected by users, Google will delete the app from its app store ecosystem and from devices that already run the app (Miller, 2011). When an app is installed on Android it will also be sandboxed. However, the sandbox technique that Android uses is very different from Apple's iOS. In contrast with the standardized sandbox technique of iOS, Android uses customized sandbox properties for each app. When the app is installed the user will get informed about the permission that the app

needs, in order to provide its full functionality. The user than has to approve this, which means that the user is deciding the level of security (Hoog, 2011). Besides controlling and preventing malicious apps on devices, a deeper level of security needs to be present as attackers can also access the device using vulnerabilities on the level of OS, browser, email, SMS or even the devices GSM radio (Weinmann, 2012). iOS uses a layered approach to defend exploits. At first two techniques, data execution prevention (DEP) and address space layout randomization (ASLR) are used to prevent executing any code on the device (Miller, 2011). DEP is a technique that distinguishes code from data. The exploit code from the attacker is identified as data and cannot be used as code in any process. Attackers mostly use return-oriented programming (ROP) to bypass this technique. With ROP an attacker uses little pieces of existing code for the exploitation (Miller, Blazakis, DaiZovi, Esser, Iozzo & Weinmann, 2012). However, when ASLR is in place, ROP can't be used as it randomized the location of code so that the pieces of code cannot be localized. If an attacker is able to execute any exploitation code, iOS has so many restrictions like sandboxing, that the attacker has very limited execution possibilities (Miller, 2011). For Android things are different, DEP and ASLR are not supported which makes it much easier to exploit code. One big advantage as stated by Miller (2011) is that most of the Android applications are written in Java, which is mostly not vulnerable for memory corruption.

Besides the security controls that are taken to prevent attacker's exploiting their code on mobile devices, both mobile operating systems have taken security measures that are protecting data when the device is physically exposed to a malicious entity. iOS configuration management helps enterprises controlling their iOS devices by distributing custom configuration files that enforce security settings. The configuration files can be created with Apple's iOS configuration utility and can be distributed with Apple's configuration utility or by third party Mobile Device Management (MDM) tools. Table 2 provides an overview of all different payload settings that are available in the configuration files (security related settings are highlighted). The standard configuration files provide limited control to iOS devices. More elaborated settings can be managed by third party MDM solutions and will be elaborated in the next section. When devices are not managed by enterprise MDM solutions, users are still able to remotely control and wipe their device using iCloud (Negrino, 2013). Encryption is another important factor of device security. With the introduction of iOS5, the data protection API was introduced. This API automates the encryption and decryption of iOS devices by letting the developer decide which data should be encrypted and with what conditions the device is allowed to decrypt (Miller et. Al, 2012). With the introduction of iOS 7 new security measures are taken. At first, 'Per app VPN' is introduced which allows organizations to setup a secure VPN for a single app. Secondly, a change to the earlier discussed data protection API is made, in earlier versions developers had to identify which data should be encrypted, with iOS 7 all app data is encrypted by default. The last and most discussed new security feature is 'Activation lock'. This feature makes stolen or lost devices unusable for malicious actors. Even when a device is completely wiped, the Apple ID credentials of the device's owner are needed to use the device (iMore, 2013).

For Android the security measures are much more complex to evaluate as there are a lot of different versions available that are also often customized by the device manufacturer. In 2013, already 550 different Android device types are available, produced by 48 different manufacturers (MaaS360, 2013). Although new security measures are introduced with new Android versions, the adoption of new Android versions is very low due to the fact that device manufacturers are responsible for distributing Google's updates (MaaS360, 2013).

Most common security measures are comparable to the measures for iOS. The password or PIN requirements can be specified, devices can be remotely wiped or locked and restriction policies can be enforced. From Android 2.2 a device administration API is provided that enables a user to set the level of security for a specific app (Hoog, 2011).

Payload	Description
Removal Password	Specifies a password that users must enter to remove a locked profile from the device
Passcode Policy	Defines whether a passcode is required to unlock the device and how complex this passcode must be
E-mail	Configures the user's e-mail account
Web Clip	Places a web clipping on the user's home screen
Restrictions	Restricts the user of the device from performing certain actions, such as using the camera, iTunes App Store, Siri, YouTube, Safari, and so on
LDAP	Configures an LDAP server to use
CalDAV	Configures a user's network calendar account using CalDAV
Calendar Subscription	Subscribes the user to a shared CalDAV calendar
SCEP	Associates the device with a Simple Certificate Enrollment Protocol server
APN	Configures an iOS device with a cellular baseband (iPhone or iPad) to use a specific mobile carrier
Exchange	Configures a user's Microsoft Exchange e-mail account
VPN	Specifies a Virtual Private Network (VPN) configuration for the device to use
Wi-Fi	Configures the device to use the specified 802.11 network

Table 2: Configuration Profile Payload Types (Miller et. Al, 2012)

Wessel, Stumpf, Herdt & Eckert (2013) present a technique that enables default Android devices to be virtualized on operating system level. The technique is developed to separate different Android environments on one device and be able to separate a corporate and private environment. Chen, Lee & Hsu (2012) introduce a new solution for mobile device security by combining an integrated biometric sensor with a password to create secure two-factor authentication. Despite the fact that users can execute tasks with different levels of needed security, authentication of mobile devices completely rely on the moment when users unlock their mobile device. Crawford, Renaud & Storer (2013) introduce a framework for transparent mobile device authentication. Their approach uses biometric technology to transparently authenticate users while using their mobile device.

Mobile Device Management (MDM)

Enterprise mobile device management (MDM) software is: (1) a policy and configuration management tool for mobile handheld devices (smartphones and tablets based on mobile OSs), and (2) an enterprise mobile solution for securing and enabling enterprise users and content. It helps enterprises manage the transition to a more complex mobile computing and communications environment by supporting security, network services and software and hardware management across multiple OS platforms. This is especially important as bring your own device (BYOD) initiatives and advanced wireless computing has become the focus of many enterprises. MDM solutions offer integrated sets of functions to manage corporate as well as private mobile devices. These functions can be categorized as device provisioning, OTA (over-the-air) configuration, certificate management, email and app management, app portal, document management, security management and expense management. (Forescout, 2013). Rhee (2012) explains the general architecture of a MDM system in five steps; see Figure 6: MDM Architecture (Rhee, 2012). In the first step the desired configurations of the mobile devices are configured, also the business users are enrolled to the MDM system. In the

second step the specified configuration is distributed to the user's device using an enterprise appstore or other in-house sharing solutions. In the third step the MDM agent sends device information as MAC addresses, IMEI number and phone number to the MDM server in order to verify the device. In the fourth step, the MDM server tells the MDM agent when certain commands as a device lock/wipe should be executed. The last step is continuous monitoring, where the MDM agent reports the device status to the MDM server.

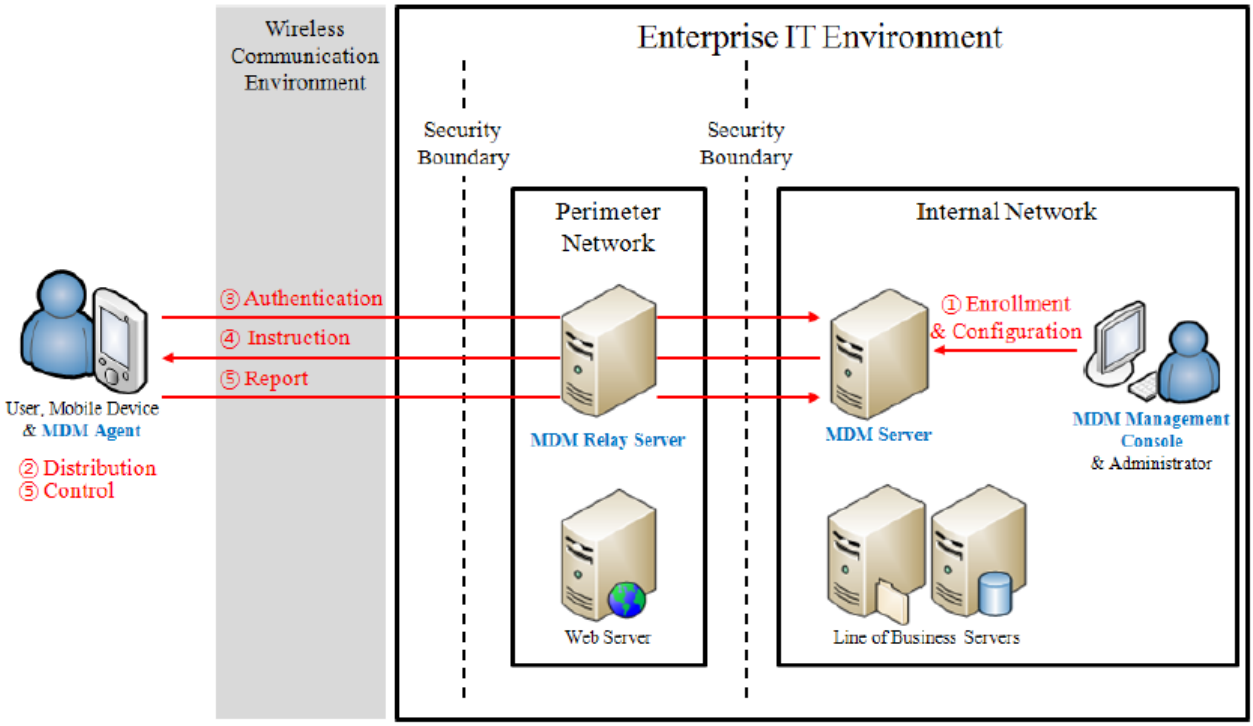


Figure 6: MDM Architecture (Rhee, 2012)

MDM systems are already becoming mature in their basic functionality. Gartner (2013) states that MDM services are expanding from traditional configurations, policy management, IT administration and reporting to deeper security with containerization, mobile application management (MAM) and mobile content management (MCM). Zenprise (2013) already makes the distinction between MDM 1.0 and MDM 2.0, where MDM 1.0 is described as a solution that enables security, governance and control measures like the configuration of the device. The difference with MDM 1.0 and MDM 2.0 is explained as that MDM 2.0 should be open in order to provide the users as much functionality as possible and still be able to secure mobility (Zenprise, 2013). Although MDM systems provide great management, security and monitoring capabilities, current systems are not able to solve more extensive security issues (Trustwave, 2013). The contribution of Ruebsamen & Reich (2012) is an alternative or in some situations an extension to a MDM system. The solution focusses on the control of mobile applications, enterprise services and internet services. The solution uses a cloud proxy that manages the access of mobile devices to the different services using Role Base Access Control (Ferraiolo & Kuhn, 2009). It enables enterprises to blacklist certain (versions of) applications of services that have known vulnerabilities or are not allowed to specified user roles.

Privacy

When taking a small side step from security, the field of privacy and regulations can be found. Seriot (2010) explains privacy with mobility as the confidentiality of personal data. Most international privacy authorities state that everyone has the right to be protected against the misuse of their personal data (CBP, 2013). Moreover, Mandujano (2012) defines privacy as '*The right individuals have to control their personal information and decide how and when they interact with others'.*

Privacy is especially complex when it comes to enterprise mobility and BYOD programs. This is because the ownership of data is often hard to identify and devices are always in different boundaries of legislation. Furthermore, the portability of mobile devices and their usage profiles make mobile devices complex assets in terms of privacy and regulation. For the millions of users, mobile devices seem to give a certain sense of privacy and also anonymity as users are sharing personal information as pictures, calendars, profile information and private messages over the internet. However, possible privacy breaches can have long-lasting effects on a personal life. Identify theft, public embarrassment, blackmail and fraud are possible privacy threats that can be very harmful and also hard to repair (Mandujano, 2013). Mobile operating system vendors as well as application developers need to become more aware of privacy issues and protect users against possible harm (Wood et Al., 2012).

Mandujano (2013) provides an approach to mitigate privacy threats on mobile hardware. The threats are organized in three categories, Personal data exposure, device identification & location and User activity. Furthermore, three different 'privacy privileges' are defined that can be used to mitigate the threats in each category as shown in Figure 7: Privacy framework: assets and privileges (Mandujano, 2013). The first privilege, 'choice' is explained as the possibility to decide which information is disclosed, collected, shared or received. The second privilege, notification, is the practice of notifying the user on how information is used. And the last privilege, control, is the ability to change how information is used by certain applications. In the first threat group, exposure of personal data, mitigating controls as Direct Memory Access and audio and camera controllers are explained (Mandujano, 2013). The 'user activity' threat group names controls as device management, embedded cores, Bluetooth disabling and BYOD policies.

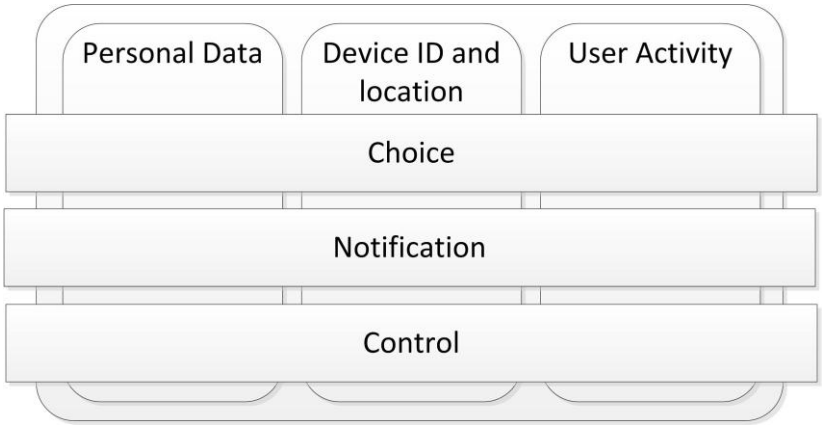


Figure 7: Privacy framework: assets and privileges (Mandujano, 2013)

Werthmann et Al. (2013) introduce a solution called PSiOS (Privacy & Security to iOS) that detects and prevents privacy breaches. The solution provides sandboxing (Greamo & Gossh, 2011) profiles for individual applications on iOS. These profiles can be configured by the user or IT administrator and consist of information usage and privacy settings. Besides controlling these settings, the tool also monitors whether an application follows the desired privacy settings. For the more open mobile operating system, Android, multiple comparable solutions are proposed. The work of Enck et Al. (2010) introduces a similar system called TaintDroid, which is a system-wide information tracking tool that tracks privacy sensitive data from all running applications. Hornyack et Al. (2011) introduce a two tiered solution called AppFence. This Android information privacy protection system shadows privacy sensitive information flows on the device and on the other hand blocks privacy sensitive information from leaving the device. They also conclude that 34% of the apps tested with AppFence do not commit with the privacy settings that where desired by the user.

3.4 IT Risk Management

In the world of IT Risk Management several renowned standards are available that have (partly) included the process of identifying risks of information systems. This chapter provides an overview of the standards that are available and used as a basis within this research. Chapter 5.3 Risk Assessment explains how these theoretical standards are used to define the Mobile Risk Assessment Method (M-RAM).

COSO

The Committee of Sponsoring Organizations' (COSO) was organized in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting. The mission (derived from their website) is stated as followed *"provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations."* (COSO, 2013). The integrated framework shown in Figure 8: COSO cube matrix (COSO, 2013) is a three-dimensional framework that explains the relation between the achievement of objective and the components of Enterprise Risk Management (COSO, 2004). The achievements of the objectives of the four entities are defined as followed:

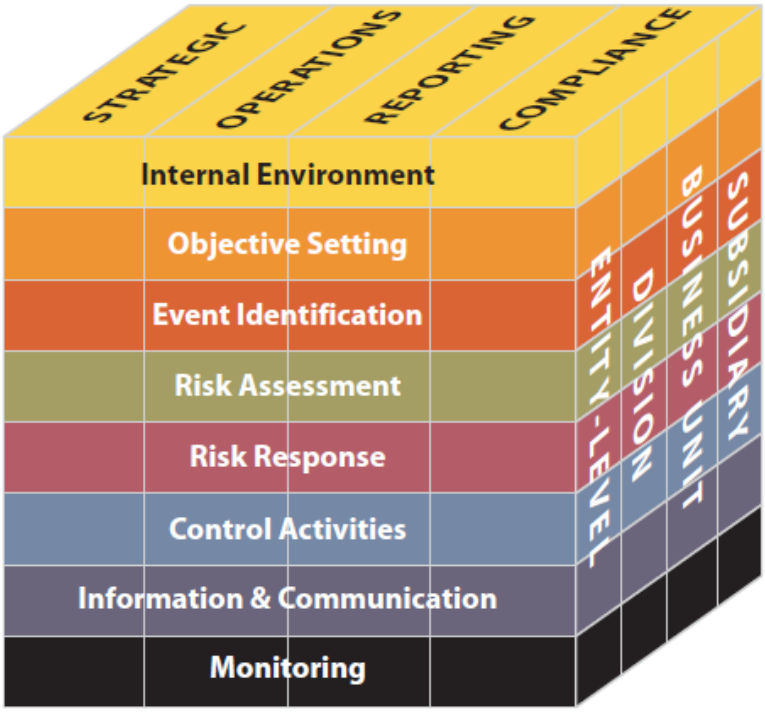


Figure 8: COSO cube matrix (COSO, 2013)

- Strategic – high-level goals, aligned with and supporting its mission
- Operations – effective and efficient use of its resources
- Reporting – reliability of reporting
- Compliance – compliance with applicable laws and regulations.

Enterprise Risk Management is defined as a set of tools for systematically identifying, assessing and managing risks throughout the value chain (Curkovic, Scannell, Wagner & Vitek (2013). The components 'Event Identification', 'Risk Assessment' and 'Risk Response' are very useful for this research. The 'Event Identification' component defines the risks that are initiated by the external environment. The Risk Assessment component states that risks need to be analyzed based on their likelihood and impact in order to define how these risks should be managed. It also states that risks should be assessed on an inherent basis, where the residual risks should be accepted. The Risk Response component identifies and evaluates possible mitigating controls to respond to the assessed risks (COSO, 2004). In addition to the COSO integrated framework, COSO published additional guidelines and risk management controls for Cloud computing (COSO, 2012). As Cloud computing has a close relation to mobile computing, this additional publication helps operationalizing the use of the integrated framework for this research.

ISACA

The history of ISACA goes back to 1967. A group of people with auditing and control background start discussing the need for a centralized organization for information guidance. In 1969 the group became known as the EDP Auditors Association, which later became ISACA (Information Systems Audit and Control Association). Nowadays, ISACA has than 110,000 members and is active in different IT governance topics (ISACA, 2013). ISACA is mostly known from their COBIT (Control Objectives for Information and Related Technology), a framework that provides an end-to-end view on the governance of enterprise IT. COBIT 5 is a set of principles, tools and models that helps guiding professionals to govern IT. COBIT 5 is based on five simple principles (ISACA, 2013):

- Meeting Stakeholder Needs
- Covering the Enterprise End-to- End
- Applying a Single, Integrated Framework
- Enabling a Holistic Approach
- Separating Governance From Management

Besides the well-known IT governance framework COBIT 5, ISACA provides several other frameworks and guidelines related to IT governance. The Risk IT framework is one of these frameworks and is especially useful within the context of this research. The framework is based on the Enterprise Risk

Figure 9: Risk IT Process Model (ISACA, 2009)

Management principles of COSO and ISO31000. In Figure 9: Risk IT Process Model (ISACA, 2009) the risk IT framework is explained. The framework exists of three main attention areas namely Risk Governance, Risk Response and Risk Evaluation. Risk Governance is explained as the practice that ensures that IT risk management is embedded in the enterprise. Risk Response is the practice that needs to address risk issues, opportunities and events in line with business priorities. The third practice, Risk Evaluation is mostly related to this research as it explains how risks should be identified, analyzed and classified. Furthermore, the IT related risks should be described so that business can understand the risks and will be able to evaluate and accept risks (ISACA, 2009). To put

the Risk IT framework in perspective, ISACA (2009) relates the framework to the Val IT framework and the COBIT IT processes, see Figure 10: Relation of Risk IT framework to Val IT and COBIT (ISACA, 2009). When the value of IT assets change due to internal or external events, the Val IT framework identifies the value of assists, which influences how IT Risks should be evaluated. The COBIT processes manage all IT related activities. The execution of these processes defines where certain risks can be identified and thus influences the risk management.

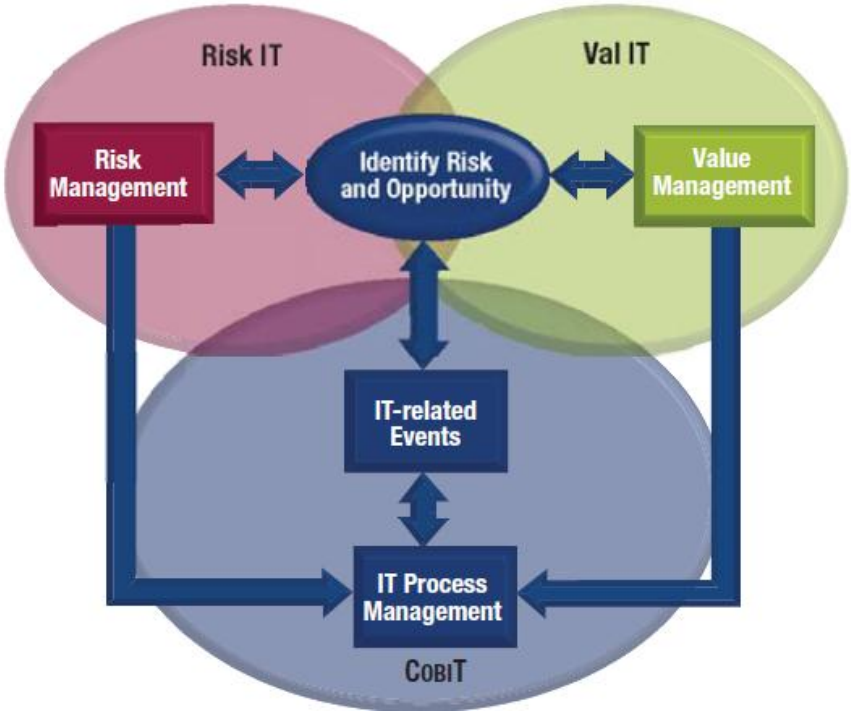


Figure 10: Relation of Risk IT framework to Val IT and COBIT (ISACA, 2009)

SPRINT

Simplified Process for Risk Identification (SPRINT) is a simple method to help business managers identify risks. SPRINT is developed by the Information Security Forum (ISF) and consists of three simple steps to identify risks. In step 1: 'assess business risks' the business manager needs to assess the business impact of a loss of the confidentially, integrity or availability of information. The second step 'Assess threats, vulnerabilities and controls', identifies the threats opposed to the assessed system, the available vulnerabilities and the controls that are in place to mitigate the risks. The last phase 'produce agreed action plan' is very general as it states that an action plan should be agreed between IT and the business. The SPRINT method is mostly used as a practical example to perform a risk analysis. There is no scientific literature that supports the success of the SPRINT method.

ISO

ISO (International Organization for Standardization) is an organization that develops international standards for different industries. ISO was founded in 1947 when engineers from 25 different countries decided to start an international organization that would coordinate international industrial standards (ISO, 2013). The official website states that nowadays 163 countries are working together to develop and maintain ISO standards (ISO, 2013). With respect to the field of this research there are two different ISO collection standards that are highly related and used. The first one is the ISO27000 family, which provides different standards for Information Technology, Information Security and Information Security Management Systems. An overview of the family is provided below (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 system 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

The ISO27005 standard will be further discussed as it is especially interesting because it is focused on information security risk management. The second related standard is the ISO31000 standard, which focuses on principle and guidelines for risk management.

The ISO27005 standard defines 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" (ISO/IEC 27005, 2008). The risk analysis process outlined in the standard indicates the need to identify information assets at risk, the potential threats, vulnerabilities and the potential impact. Unfortunately, the standard does not pride any possible methods to execute a risk assessment. The standard does provide a high-level three step approach to information security risk management as shown in Figure 11: High-level information security risk management (ISO/IEC 27005, 2008).

Figure 11: High-level information security risk management (ISO/IEC 27005, 2008)

Furthermore, the standard provides examples of threats, vulnerabilities and impacts. It is clearly implied that automated system security vulnerability assessment tools are insufficient for risk analysis without taking into account other vulnerabilities plus the threats and impacts: "merely having certain vulnerabilities does not necessarily mean your organization faces unacceptable risks if the corresponding threats or business impacts are negligible in your particular situation." (ISO/IEC 27005, 2008).

ISO31000 provides guidelines and principles on how to manage any kind of risks an organization has to deal with. The standard provides a risk management process (Figure 12: Risk Management process (ISO31000, 2009)) that can be used as a guideline for risk management. The blue square in the center of Figure 12 represents the risk assessment and consists of three steps.
In the first step, risk identification, the sources of risk, areas of impacts and events are identified based on their cause and potential consequences. Internal as well as external triggered risks should be included. The output of this step should be a list of risks based on events that might create, enhance, prevent, degrade, accelerate or delay the execution of business objects. The standard also states that risk identification tools and techniques should be used as well as knowledgeable people to perform the risk identification step.
ISO31000 (2009) explains the risk analysis step as a practice where the risk needs to be understood, and if and how a risk should be treated. For each identified risk, the positive and negative consequences (impact) and the likelihood that those consequences can occur need to be determined. The standard does not provide any methods to perform this analysis, but states that the confidence of determination on the level of risk and used method should be communicated to the

risk decision makers. The last step, risk evaluation assists in making decisions on the risk analysis outcome. During the evaluation a prioritization of treatments should be made based on the risk analysis, organizations benefits, and legal, regulatory requirements.

The steps that are not part of the risk assessment (Communication and Consultation, Establish Context, Risk Treatment, Monitor and Review) are not further explained as they are self-explanatory and not in the direct scope of this research.

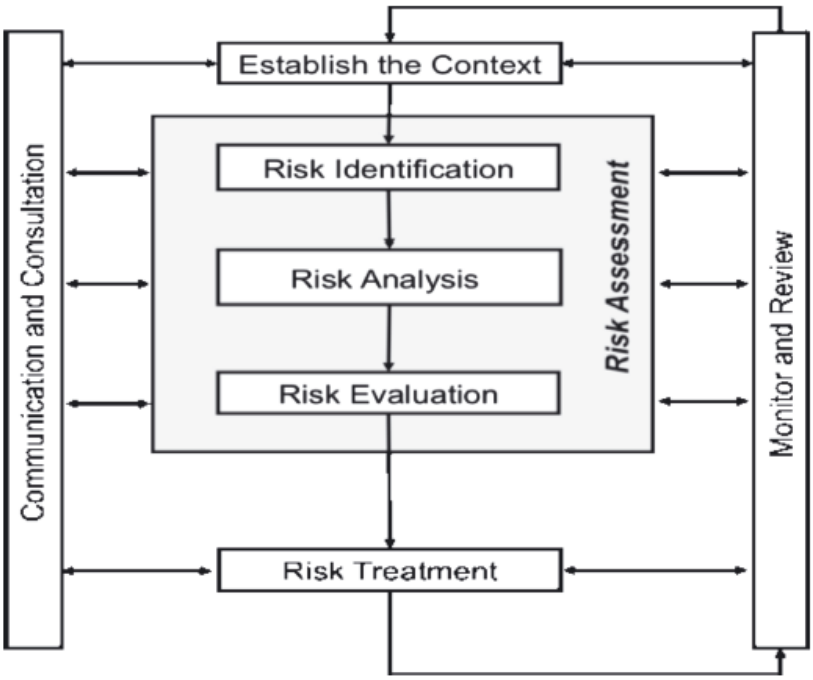


Figure 12: Risk Management process (ISO31000, 2009)

IRAM

The ISF (Information Security Forum), founded in 1989, is an independent organization that focuses on investigating, clarifying and resolving issues in information and risk management. The ISF security model gives a good understanding of the elements that are part of the forum. Figure 13: ISF Security Model (ISF, 2013) shows how the different elements are supported with knowledge exchange, research methods and tools & methods (ISF, 2013). The green highlighted triangle 'risk' provides the IRAM (Information Risk Assessment Method) method. The method helps organizations identify, analyze and manage information risks. The method is based on more than ten years of research and practices from leading organizations.

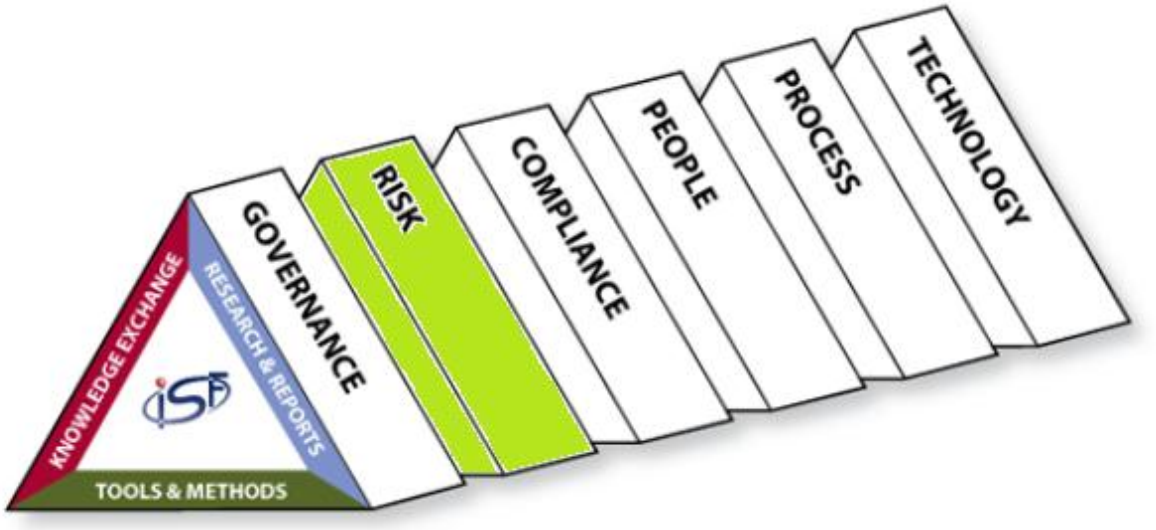


Figure 13: ISF Security Model (ISF, 2013)

The IRAM method consists of three phases (ISF, 2013);

1. Business Impact Assessment (BIA) which determines which applications are most critical for an organization (confidentiality, integrity, availability).
2. The Threat & Vulnerability Assessment (TVA) which determines what threats have an impact on the BIA rated systems and how known vulnerabilities can exploit that threat. Next, the assessment produces a likelihood rating which, together with the BIA rating, determines the risk score.
3. The Control Selection (CS), which determines what controls need to be in place to mitigate the defined risks.

During these phases a list of 49 key information risks is used as a basis for the assessments. The 49 information risks are divided over the following categories;

- External attacks
- Internal misuse and abuse
- Theft
- System malfunction
- Service Interruption
- Human error
- Unforeseen effects of change

User guide

Business Impact Rating

Integrity

Ref.	Business impact type *Business impact of errors in information or of deliberate manipulation of information to perpetrate or conceal fraud (most serious case)*	Business impact rating A-Very high, B-High, C-Medium, D-Low, E-Very low				
		A	B	C	D	E
Financial						
F1	Loss of sales, orders or contracts	20% +	11% to 20%	6% to 10%	1% to 5%	Less than 1%
					X	
F2	Loss of tangible assets (eg fraud, theft of money, lost interest)	$20m+	$1m to $20m	$100K to $1m	$10K to $100K	Less than $10K
						X
F3	Penalties/legal liabilities (eg breach of legal, regulatory or contractual obligations)	$20m+	$1m to $20m	$100K to $1m	$10K to $100K	Less than $10K
					X	
F4	Unforeseen costs (eg recovery costs)	$20m+	$1m to $20m	$100K to $1m	$10K to $100K	Less than $10K
					X	
F5	Depressed share price (eg sudden loss of share value)	25% +	11% to 25%	6% to 10%	1% to 5%	Less than 1%
						X

Figure 14: BIR Integrity example (ISF, 2013)

The BIA phase starts with a form to define the BIRT (Business Impact Reference Table). This table defines five levels (Very high – Very low) of impact that can be measured in the amount of loss in finance, operations, employees or customers. Than a system profile is defined that explains the assessed object in detail. After these steps are finished, the actual assessment is conducted. A BIR (Business Impact Rating) on Confidentiality, Integrity and Availability is performed. Each BIR is evaluated using the defined BIRT references. An example of a BIR is shown in Figure 14: BIR Integrity example (ISF, 2013). The last step of the BIA phase is the creation of a BIA summary, which provides an overview of the total BIA assessment score.

The TVA phase uses the same system profile as the BIA phase, in order to scope the assessed system. Then ISF states that the assessed system (asset) should be understand in terms of system conditions, linked systems, tools, forms and participants that will be part of the assessment. After concluding these preliminary activities the threat assessment is conducted. The assessment exists of two parts, (1) the determination of applicable threats and (2) assessing the factors that affect the threat rating. The assessment tool provides 49 possible threats (E.g. 'Hacking', 'Cracking passwords', 'Eavesdropping' and 'User errors') that

Likelihood Reference Table

Using the Likelihood Reference Table

The **Likelihood Rating** for a particular threat (ie the likelihood of an information incident occurring) can be determined by looking up the value in the **Likelihood Reference Table** (below) that corresponds to the **Overall Threat Rating** and **Overall Vulnerability Rating** (from the Vulnerability Assessment form).

Overall Vulnerability Rating		Overall Threat Rating: Very Low	Low	Medium	High	Very High
Very High	A	D	C	A	A	A
High	B	E	C	B	A	A
Medium	C	E	D	C	B	A
Low	D	E	D	D	C	C
Very Low	E	E	E	E	E	D

Save table | Save as... | Reset table | Close

Figure 15: Likelihood Reference Table (ISF, 2013)

need to be assessed on their applicability (1) and how factors (i.e. internal, external) affect (low, medium, high) a threat (2). With the vulnerability analysis the 49 threats are assessed on known environmental, system and technical vulnerabilities. Each threat is determined on a scale from very low till very high, resulting in an overall vulnerability rating. The next step is determining the likelihood rating. By combining the overall threat ratings and the linked vulnerability ratings, a likelihood rating can be determined using the likelihood reference table (Figure 15: Likelihood Reference Table (ISF, 2013)). In the last step of the assessment the information risk rating is determined. Based on the information risk reference table (BIA vs. Likelihood) an overall information risk rating is determined.

The last phase (CS) defines and evaluates controls to mitigate the determined risks. The first step is to fill in the key information risk from, which incorporates the output of the TVA phase (information risk rating), the affected CIA properties and explanatory comments on each information risk. The next step is the control evaluation step, where a list of available and possible controls (this list needs to be available or created at the risk department) is evaluated on their applicability for the defined risk. Example controls are 'Intrusion detection', 'System monitoring', 'Cryptographic solutions' and 'Public Key Infrastructure (PKI)'. The last step of the CS phase is to determine which controls should be required in order to mitigate the evaluated risks appropriately. The method also provides a System Risk Action Plan that can be used to follow up possible actions after conducting the risk analysis.

Overall, the IRAM method is a very practical method with an extensive collection of practical forms and description how to conduct the risk analysis.

NIST

The National Institute of Standards and Technology (NIST) was founded in 1901 by the U.S congress. NIST was originally organized to create a more competitive measurement infrastructure for the U.S, compared to other organizations around the world. Nowadays NIST has measurement standards that support all kind of technology practices (NIST, 2013). The NIST has two standards that are related to risk assessment. The NIST Special Publication 800-39 is a publication on managing information security risk and part of the information security family (Aroms, 2012). The NIST Special Publication 800-30 is also part of the information security family and provides guidelines on conducting a risk assessment (Aroms, 2012). Figure 16: Risk Management Process (Aroms, 2012) shows how the 800-39 publication defines the risk management process. The framing component in the middle of the framework is used to define the risk strategy of an organization. Intend to assess risks, respond to risks and monitor risks are part of the risk strategy framing. The risk frame should at least contain of the following components (Aroms, 2012):

- Risk assumptions (e.g., assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time)
- Risk constraints (e.g., constraints on the risk assessment, response, and monitoring alternatives under consideration)
- Risk tolerance (e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable)
- Priorities and trade-offs (e.g., the relative importance of missions/business functions, trade-offs among different types of risk that organizations face, time frames in which organizations must address risk and any factors of uncertainty that organizations consider in risk responses)

The 'assess' step of the risk management process is highly related to this research as it defines the process of assessing risks related to a certain object. The following parts should be identified during the assess process (Aroms, 2012):

1. Threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation
2. Vulnerabilities internal and external to organizations
3. The harm (i.e., consequences/impact) to organizations that may occur given the potential for threats exploiting vulnerabilities
4. The likelihood that harm will occur.

The result of this identification should be a determined risk, or in other words the likelihood that a certain risk will occur. The standard also defines a list of input and tools that is used to perform the assessment. These will be further elaborated in the 800-30 publication of NIST (Aroms, 2012).

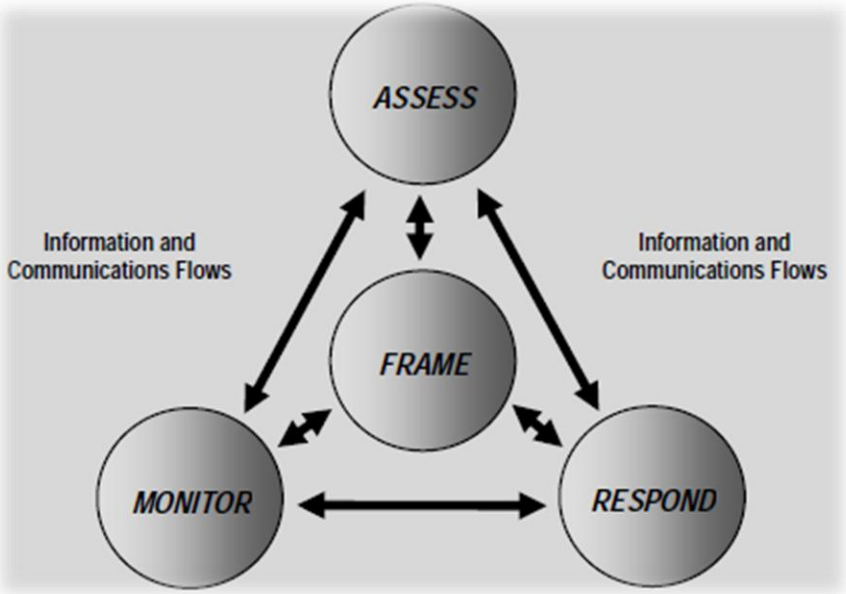


Figure 16: Risk Management Process (Aroms, 2012)

The respond process explains how the organizations should respond to risk incidents and the monitor process explains how possible threats and incidents can be monitored and detected. These steps are not further elaborated as they are not in scope of this project.

The 800-30 special publication focusses on the assessment component of risk management. Preparing, conducting, communicating and maintaining a risk assessment is central in the 800-30 publication (Aroms, 2012). The publication starts with explaining that a risk assessment is not a one-time event but rather a recurring event during the life-cycle of an information system. The key concepts used with a risk assessment are extensively explained. A brief summary of each concept is provided below;

- Risk – *"a measure of the extent to which an entity is threatened by a potential circumstance or event and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."*
- Information risk – focused on the loss of confidentiality, integrity and availability of information.
- Risk assessment - the process of identifying, estimating, and prioritizing information security risks.
- Risk assessment methodology – consist of an assessment process, risk model (relation between risk factors) and assessment approach.
- Threats - any circumstance or event with the potential to impact organizational operations and assets.
- Threat source – the method that is used to (un)intentionally exploit a vulnerability.

- Threat shifting – the activity of minimally changing the threat source in order to bypass safeguards or mitigating controls.
- Vulnerability – *"a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source".*
- Predisposing condition – a condition that increases or decreases the likelihood of a threat.
- Likelihood of occurrence – the probability that a threat is capable of exploiting a vulnerability.
- Impact – the harm that can be expected from a certain threat.

The relation between these key aspects can be explained using a generic risk model as shown in Figure 17: Generic risk model (Aroms, 2012).

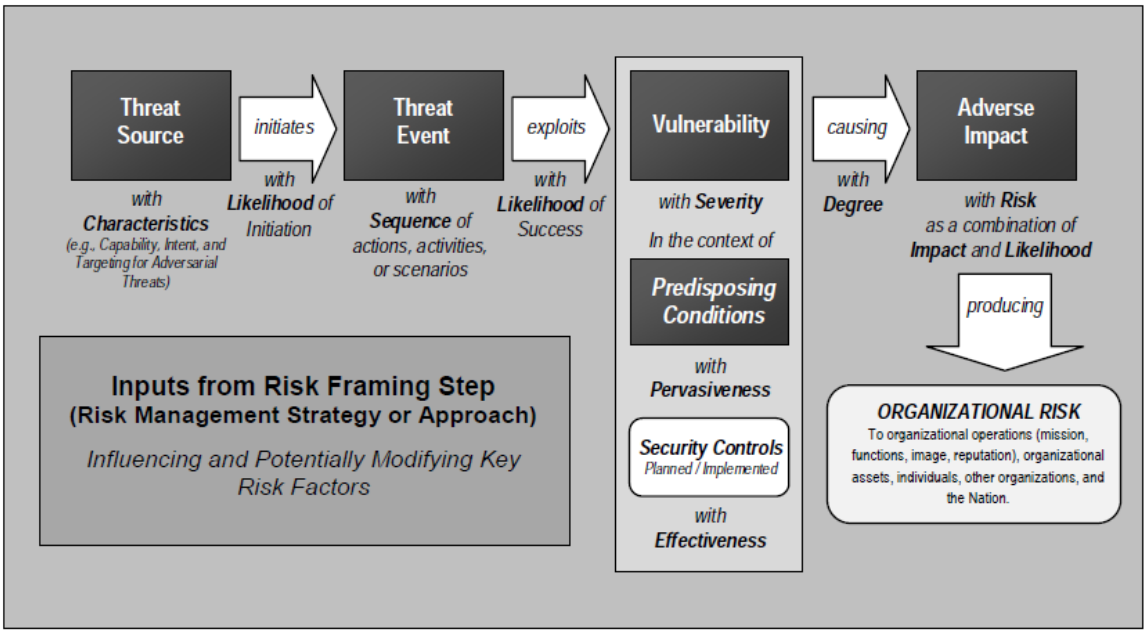


Figure 17: Generic risk model (Aroms, 2012)

After defining the key risk concepts, the publication provides a detailed risk assessment process (Figure 18: Risk assessment process (Aroms, 2012)). The first step explains how the assessment should be prepared. The identification of the purpose, scope, constraints, information sources and approaches/analytics of the assessment are the core of the first step. The second step is the execution of the assessment and contains out of five sub-steps. First the threat sources (e.g. hacker, trusted insider) and threat events (e.g. DoS attack, phishing) need be identified. Then the vulnerabilities, predisposing conditions of the assessed system and its environment are identified. The publication provides a table with common predisposing conditions (e.g. architectural decisions). During the third sub-step the likelihood of occurrence is determined (Several quantitative assessments for likelihood are provided in the publication). Sub-step four determines the magnitude of impact for a certain risk. Within this sub-step three conditions are evaluated, (1) the characteristics of the threat that could initiate the threat, (2) the identified vulnerabilities and (3) the implemented safeguards or mitigating controls. The last sub-step of the assessment is the determination of risk caused from each threat, based on the impact and likelihood (Aroms, 2012). The third step explains how the results of the risk assessment should be communicated to the organization and the risk decision makers. Furthermore, a fourth step is explained to monitor changes of assets, IS components, the organization or individuals that can possibly influence the risk assessment outcome.

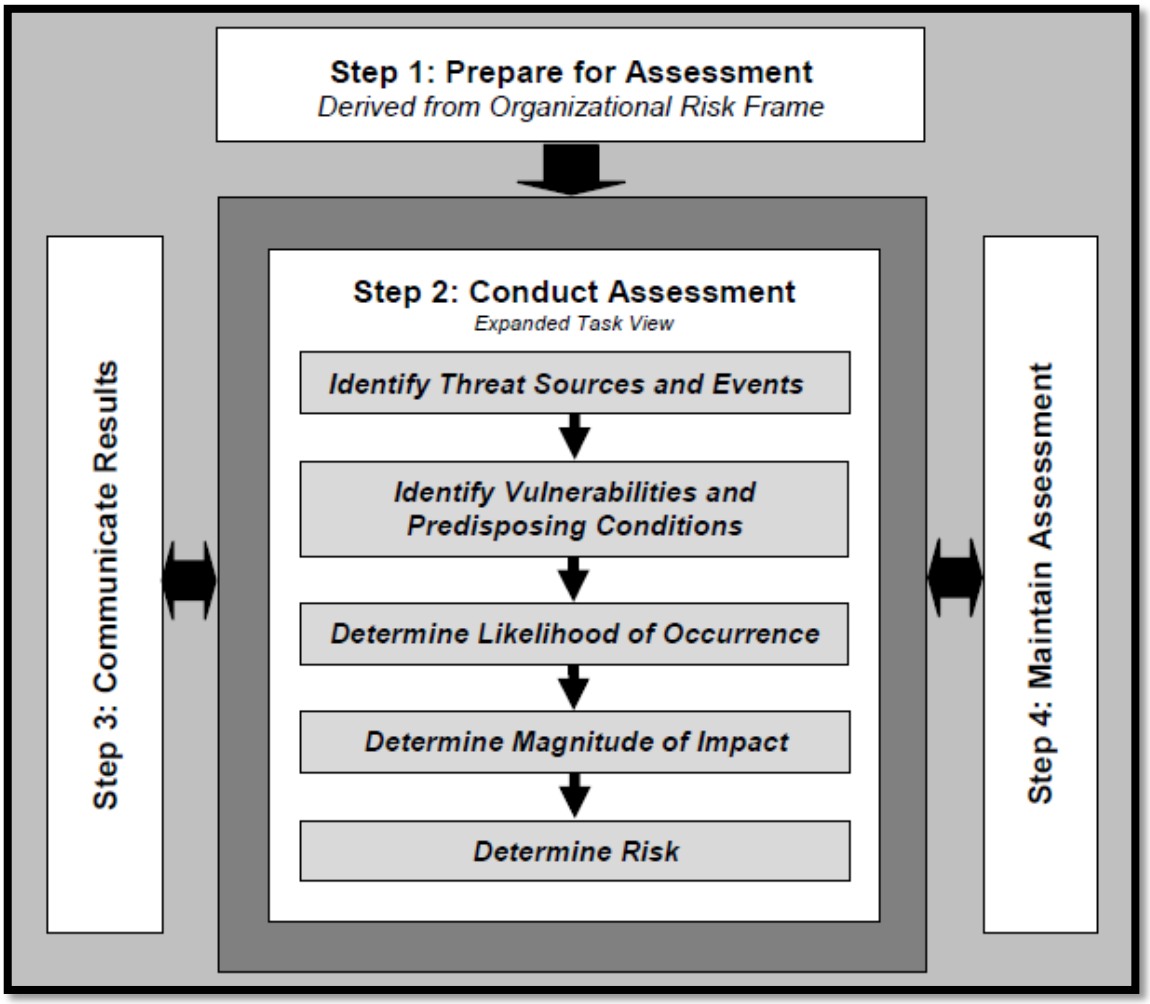


Figure 18: Risk assessment process (Aroms, 2012)

OCTAVE

The CERT (Computer Emergency Response Team) provides a standard called OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). The standard is a risk-based strategic assessment technique for security. The standard has a more business than technology-centric view on security risks (CERT, 2013). The OCTAVE method uses workshops with people from different levels in the organization. These workshops are focusing on the following information (CERT, 2013)

- Identifying critical assets and the threats to those assets
- Identifying the vulnerabilities, both organizational and technological, that expose those threats, creating risk to the organization
- Developing a practice-based protection strategy and risk mitigation plans to support the organization's mission and priorities

Beside the OCTAVE method, there is also a simplified version for smaller companies (OCTAVE-S) and a more comprehensive guideline (OCTAVE-Allegro) that defines the process of risk assessing and assurance (Caralli et. Al, 2007). The OCTAVE method consists of seven processes divided over three phases. The first phase is creating asset-based profiles, where information on vulnerabilities, security assets, concern areas and current protection strategies is determined and consolidated into threat profiles (Alberts & Dorofee, 2001).This step contains the first four processes;

1. Identify Senior Management Knowledge
2. Identify Operational Area Management Knowledge
3. Identify Staff Knowledge

4. Create Threat Profiles

The second phase (Identify Infrastructure Vulnerabilities) is focused on the technological vulnerabilities that apply to the identified assets. Phase two contains the next two steps;

5. Identify Key Components
6. Evaluate Selected Components

The last phase evaluates identified risks to critical assets and defines mitigating plans for these risks. Process seven and eight are part of this last phase;

7. Conduct Risk Analysis
8. Develop & select Protection Strategy

Step seven 'conduct risk analysis' is especially interesting for this research and therefore explained more elaborate. The aim of the process is to build a risk profile for each critical asset, which is the already determined threat profile with an extension on the impact of the threat. The first activity is to identify the actual impact of a threat to the organization. The second activity is the creation of risk evaluation criteria in order to be able to identify a risk on low, medium and high impact. In the last step the outcome of the first activity is evaluated on the criteria defined in the second activity and each risk is thus evaluated on its impact.

3.5 Research Gap

The theory section provides a broad understanding on mobility, the security issues and solution for mobility as well as a deep understanding of risk assessment methodologies. It seems that the security measures for enterprise mobility are various and pinpointed to different vulnerabilities and possible threats. However, the broad spectrum of risk management and risk assessment methodologies do not provide any specifications or best practices regarding enterprise mobility.

This results in a clear gap between ad-hoc immature mobile security measures and the extensive mature risk assessment methods for traditional information systems. The existence of this gap should worry information security scientists as well as business professionals that carry the responsibility of risks that originate from enterprise mobility.

Resulting from the identified research gap, this study will focus on the development of a risk assessment method that is especially designed to identify the (residual) risks that originate from enterprise mobility. The main process of this method should be based on the risk assessment theory explained in section 3.4 IT Risk Management and the gained insight from mobile security experts & mobile security managers.

4 Empirical Findings

This chapter follows step 5 of the research process described in section 2.2 Research Process. In order to verify the problem statement of this research and be able to form a basis in answering the stated research questions, persons in different roles in the field of mobile security are interviewed. The interviews were conducted following the described method in section 2.4 Expert Interviews.

4.1 Interview Criteria

The interviewed persons are divided over two groups, Mobile Security Managers and Mobile Security Experts. The MSM's can be explained as persons within an enterprise organization that are responsible for the security of mobile devices and/or the risks that originate from the usage of mobility. The selections of the interviewees for this group are based on the following criteria:

- **Size of the organization**, minimal 1000 employees, preferable more than 10.000. This criterion is added because large organizations often have to deal with a more diversified mobile environment and targeted threats. Furthermore, smaller organizations are not using or considering the full potential of mobility due to limited resources and lacking mobile awareness (Keyes, 2013).
- **Industries,** organizations from different industries are selected in order to make the delivered artifact of this research usable in each industry. The complete selection is detailed in Table 3: Mobile Security Managers provides a selection of the included industries.
- **Expected challenges,** based on the core business of an organization and available knowledge from experienced consultants, organizations are assessed whether they have or could have interesting challenges regarding mobile security or risk management.
- **Role,** as mobile security is a new field of research it is also a new practice within organizations. Therefor finding the right person that is responsible for mobile security & risk management can be very challenging. The responsible role varied from security manager to chief information officer.

Most interviewees were not allowed to use their name and company name for any public publications. Therefore a reference structure (MSM01 – MSM10) is used to quote the interviewees. Furthermore, Table 3: Mobile Security Managers provides the industry and size of the organizations, and the role of the interviewee within its organization.

Reference	Industry	Employees	Role of interviewee
MSM01	Government	5000 – 10.000	Manager Mobile Initiatives
MSM02	Oil & Gas	50.000 – 100.000	Team lead security controls
MSM03	Chemicals	10.000 – 50.000	Mobile Security Manager
MSM04	Private Banking	1000 - 5000	Mobile Security Manager
MSM05	Banking	10.000 – 50.000	Risk assessment manager
MSM06	Telecom	10.000 – 50.000	Mobile Security Manager
MSM07	Government	10.000 – 50.000	Security Officer
MSM08	Finance	1000 - 5000	Mobile Security Manager
MSM09	Accountancy	5000 – 10.000	Chief Information Officer
MSM10	Transport	10.000 – 50.000	Mobile Risk Manager

Table 3: Mobile Security Managers

The MSE's have more diversified roles compared to the MSM's. Each MSE is an expert in the field of mobile security or risk management, but can have very different expert knowledge. Three different expert fields can be identified, (1) the mobile security expert that consults organization on how to secure mobile devices, (2) the MDM expert that implements mobile device management systems and (3) the mobile risk expert that consults organizations on how to mitigate the risks that originate from mobility. The selection criterion for the MDM experts is based on the magic quadrant of Gartner (Redman, Girard, and Basso, 2012). The quadrant leaders (MobileIron, Airwatch, Zenprise,

Fiberlink, Good Technology) were contacted and asked to contribute to this research. Both MobileIron and Zenprise co-operated and are part of the interviewed MSE's. The mobile security and mobile risk experts are selected based on related publications, existing contacts or contacts of Deloitte colleagues. Moreover, internal Deloitte experts are also added to the list of MSE's.
In order to value the knowledge and statements of the MSE's their experience in their specific field of knowledge is added in Table 4: Mobile Security Experts. A comparable reference structure (MSE01 – MSE12) is used to quote the interviewees. Furthermore, Table 4: Mobile Security Experts provides the industry and name of the expert's organizations and the role of the expert.

Reference	Industry	Organization	Experience	Role
MSE01	Research	European Network for Cyber Security	9 years (information security)	Mobile Security expert
MSE02	Information Technology	Zenprise by Citrix	8 years (mobile security)	MDM expert
MSE03	Consulting	Trustwave	14 years (security)	Mobile Risk expert
MSE04	Information Technology	MobileIron	2 years (MDM)	MDM expert
MSE05	Consulting	MiTE	5 years (MDM)	Mobile Security expert
MSE06	Research	Ernst & Young	1 years (mobile security)	Mobile Risk expert
MSE07	Consulting	Deloitte Security & Privacy	7 years (mobile security	Mobile Security expert
MSE08	Consulting	Deloitte Security & Privacy	10+ years (security)	Mobile Risk expert
MSE09	Consulting	Deloitte Security & Privacy	10+ years (security)	Mobile Risk expert
MSE10	Consulting	Deloitte Security & Privacy	10+ years (security)	Mobile Risk expert
MSE11	Consulting	iCentre	5 years (mobile security)	Mobile Security expert
MSE12	Consulting	Deloitte Security & Privacy	10+ years (security)	Mobile Risk expert

Table 4: Mobile Security Experts

For both the Mobile Security Manager as well as the Mobile Security Expert interviews, the interview protocol discussed in section 2.4 Expert Interviews is used to conduct the interviews.

4.2 Results

After summarizing the interviews, the results of the expert interviews are grouped in different subjects. The stated questions regarding each subject are explained as well as the analysis and conclusion of each subject. When possible the results of a particular subject or part of a subject are visualized. Each subject concludes with the exact statements of each interviewee, regarding the discussed subject. The following enumeration provides an overview of the topics that are discussed and explains why each topic is discussed.

- **Mobile drivers**, the experts are asked what an organization drives to use mobility in order to understand why mobility is used and how important mobility is to the organization.
- **Providing, using and supporting mobile devices**, the experts are asked how mobile devices are provided, used and supported in organizations to understand how organizations manage and use devices, and be able to understand where possible risks can originate.
- **Tension field between mobile innovation and mobile security**, it is important to know how and if experts see this tension field as it can result in less security controls to perceive mobile usability and innovation possibilities.
- **Usage monitoring,** the experts are asked if organizations monitor device, app and content usage. It is important to know what is monitored in order to understand how much knowledge organizations have on the actual usage of employees and possible threats that arise from this usage.
- **Mobile threats,** the experts are asked to determine what threats are opposed to organizations in order to understand the different mobile threats and be able to know how these threats should be identified.
- **Risk assessment & acceptance,** the experts are asked how mobile risks are assessed and if they are accepted within organizations. This question is asked to determine how mobile risks should be assessed and to understand how mature organizations are in mobile risk management.
- **Controls & MDM,** the experts are asked if organizations explicitly link controls to threats or vulnerabilities in order to understand how controls can be linked and if organizations consider the relation between threats/vulnerabilities and controls. Furthermore, the experts are asked if and how MDM solutions are used to understand if MDM systems are really used and what the added value of these systems is.
- **BYOD impact,** the experts are asked is BYOD programs exist within organizations and how the introduction of such a program impacts an organization. This question is asked to understand the impact, threats, vulnerabilities and needed controls when a BYOD program is in place.
- **Artifact components,** the experts are asked to evaluate a concept of the M-RAM (Mobile Risk Assessment Method) in order to validate the different components of the concept method.

Mobile drivers

The interviewed managers are asked on behalf of their organization what their most important drivers are for using mobile devices. The mobile experts explained what the most important drivers are for their clients. Each interviewee provided a classification of drivers to achieve with mobility. The most important driver is valued with three points, the second with two points and the third with one point. If an interviewee provides more than three drivers the less important are all valued with one point. The following drivers are ranked in Figure 19: Drivers for mobile device usage

- Productivity
- Location independent
- Answer personal's demand
- Keep up with technology
- Progressive image
- Cost reduction
- Serve clients or partners

The percentages in Figure 19: Drivers for mobile device usage are based on the total given points per category by the MSM and the MSE.

Conclusion: Managers often combine productivity with location and time independent working as a main driver. Furthermore, most experts and also a number of managers provide mobility to answer the demand of their employees. Supporting the primary process and enabling a progressive company image is also a driver that is often named by managers, but not seen by experts.

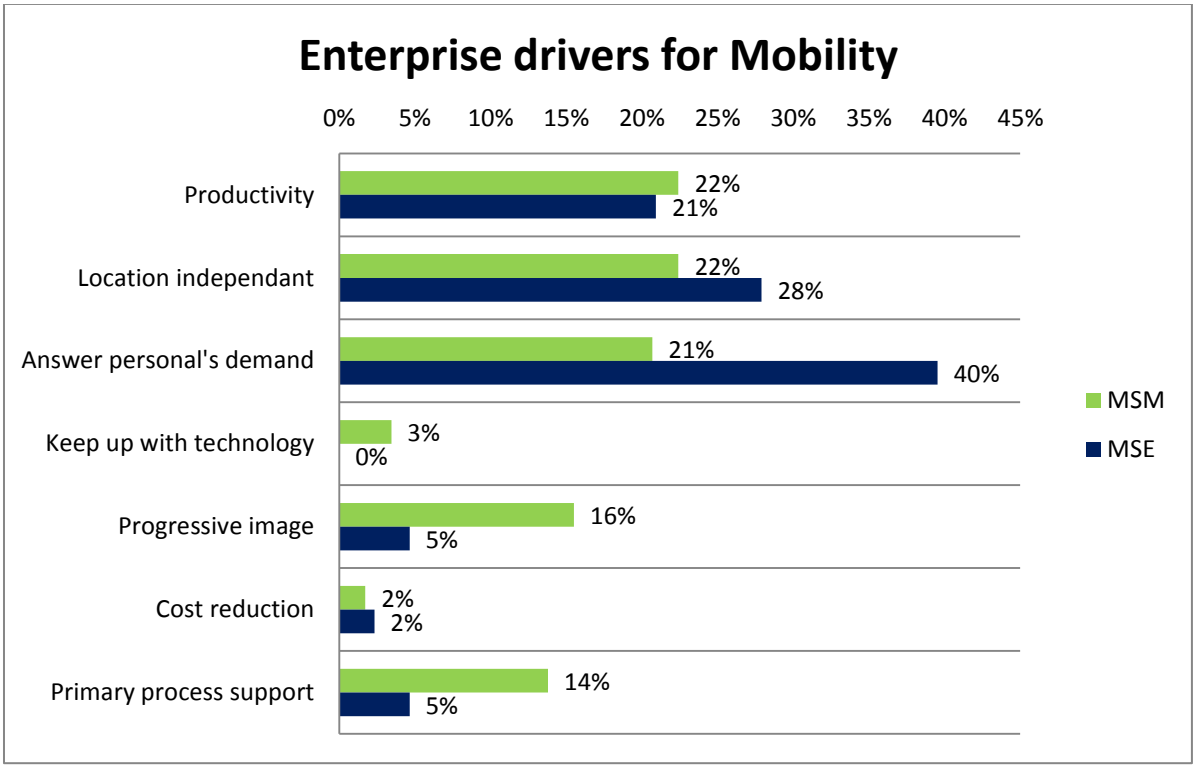


Figure 19: Drivers for mobile device usage

MSM01: "Our personnel are always traveling, mostly by train, so we want to be able to facilitate our personnel so that they can also work while traveling. So being more productive and location independent are the main drivers for mobility. Furthermore, we want to be a progressive company and also answer the demand of our employees."

***MSM02**: "We think it is very important that users can use their own devices & applications as they are already familiar with these and thus more productive. The second important driver is to keep up with the consumer market. If you keep waiting it becomes harder and harder to connect consumer devices on business systems. Furthermore, our BYOD program is used to cut cost because devices are now paid by the employees."*

***MSM03**: "The most important driver is working more productive, but also enabling personnel to work location and time independent is important. There is also a relationship between these drivers as personnel become more productive when they are able to work at home and while traveling."*

***MSM04**: "Answering personnel's demand is the most important driver and also providing the ability to work location and time independent. Tablets are used when giving presentations and sharing documents during meetings."*

***MSM05**: "Mobility is two-sided: in the first place enabling the consumer to use our services mobile is the most important. The other side is enterprise mobility, were we have the goal to work 30% of our working time outside of the corporate office. This goal is set in order to work location independent and be more productive."*

***MSM06**: "The ability to work location and time independent is a big driver, but more important is our corporate image. As we are in the mobile business, we need to be up front regarding mobile usage."*

***MSM07**: "Being more efficient and productive is the main driver, but also supporting our primary process. In court there are so many files to process and we use mobile devices (tablets) to make this process easier. A third important driver is our corporate image, it is really hard to attract the most intelligent employees and keep them within your organization. By supporting mobile extensively we try to be an attractive employer."*

***MSM08**: "The most important driver is productivity. We want to be location and time independent, which will also blur the line between private and business. A second important driver is trying to be an attractive employer."*

***MSM09**: "In the first place it is improving and maintaining our corporate image. We need to show the world that we are always upfront with technology and that we are able to realize anything. The second driver is answering employee's demand, our employees want to work where and whenever they want, office hours don't exist anymore. Furthermore, being more productive is also a driver, but not as important as the first two."*

***MSM10**: "The main driver is satisfying employees demand; we were caught up by reality as people started experimenting with mobile devices and services. Furthermore, supporting our primary process becomes more and more important and mobile dependent."*

***MSE01**: "Most companies are still trying to answer the demand of higher management. Furthermore, I think that companies are trying to gain productivity by enabling their employees to work location independent."*

***MSE02**: "In the first place it isn't drivers that you would like to see and that you would expect to be. Mostly it is making their boss happy so that he can use his iPad and insuring that employees are accessing the network on a secure way. It was more about security the last years, nowadays it's more about usability and letting users use requested apps in a secure way. It's more about supporting users in the tool they want to use, than insuring location independent working."*

***MSE03**: "Two perspectives: the employees and companies. The demand is overlapping but also different and that is where the problems arise. Companies see it as providing tools for their employees and allowing them to work when they are out of the corporate environment and allowing them to work in non-office hours. People that have mobile devices tend to work more hours and are thus more productive."*

***MSE04**: "Productivity, but also answering the demand of employees so that the company remains attractive to work for. Being able to work location and time independent mostly answers the demand of the employees. Secondly, nowadays companies are looking to make primary processes simpler by using mobile solutions. For instance, field workers that normally had to come back to the office in order to register their working hours can now use their mobile device on the location itself. A third driver is cost reduction; companies are more and more replacing expensive laptops for tablets. Tablets have way less management, support and licensing costs compared to laptops."*

***MSE05**: "The main drivers for companies are working location independent but also just answering the demand of their employees."*

***MSE09**: "For most clients the main drivers are working location and time independent. Productivity is mostly a side effect and often named as a driver."*

***MSE10**: "Most organizations use mobility in order to work location and time independent. Furthermore, managers often indicate that they try to create a progressive company image by supporting mobility."*

***MSE11**: "There are roughly three classes of mobile usage, (1) simple ActiveSync usage to answer employee demand, (2) clients that want to support their primary process by executing tasks on the go using a mobile device and (3) clients that want to use mobility for supportive processes as meetings, presentations and ERP disclosure.*

Providing, using and supporting mobile devices

The interviewed managers stated how their organization provides, uses and supports mobile devices, where the experts explained what they currently see in the market on providing, using and supporting mobile devices. Each provided answer counts equally in Figure 20: Providing, using and supporting Mobile Devices and is assigned when applicable.

Providing mobile devices:

- Full BYOD (Provide): All personally owned devices are allowed to bring to work for business use.
- BYOD with restrictions (Provided): Employees bring their own device, but only allowed devices are accepted.
- CYOD (Provided): The organization provides a list of devices where the employee can choose from.
- Company provided (Provided): The organization chooses the mobile device that is used.

Using mobile devices:

- Supporting processes (Used): Mobile devices are used for supporting processes (Mail, calendar).
- Primary processed (Used): Mobile devices are used to execute primary processes.

Supporting mobile devices:

- Helpdesk (Support): There is a helpdesk that supports users in their mobile usage.
- No support (Support): There is no support when a user has problem with its device.

Conclusion: The biggest conclusion on this research part is that BYOD is not really happening. Despite the numerous publications on BYOD and BYOD management, organizations as well as experts are not enrolling or supporting real BYOD. CYOD or tightly managed (only few devices allowed) BYOD is much more enrolled together with old fashioned 'company provided' models. On usage level all companies use mobile devices for supportive processes and some are setting up or already having support for their primary process.

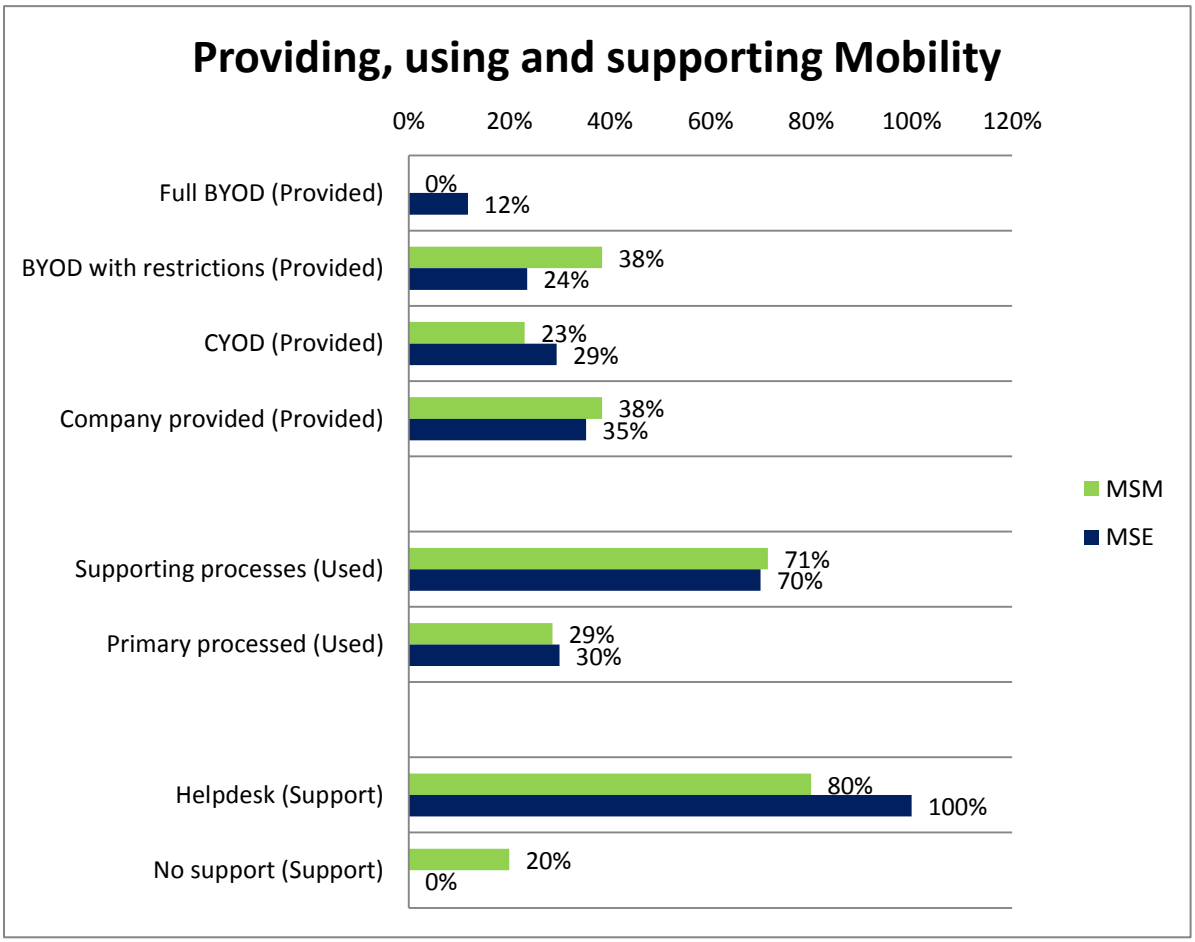


Figure 20: Providing, using and supporting Mobile Devices

MSM01: "Last year we conducted a research to determine how mobile devices could support our primary process and improve our productivity. Based on the results of that research a device selection project was executed to determine which device was best suitable for our demand. Finally, one device was selected that was able to support all processes. This device is provided to employees and owned by the organization. A BYOD program will likely not be enrolled as devices need to be specifically designed and managed in order to support the primary process. Support is still very hard to say as there is nothing arranged at the moment. Users are responsible for their own device and need to solve their own problems. This will probably be different in the future."

MSM02: "We have a BYOD environment where employees are allowed to bring Android and iOS devices that are running OS versions that are approved by our policy. We are using VOIP to communicate and employees are also allowed to declare any cost outside of their carrier contract. An MDM solution manages a corporate environment on every device. The devices are used for supportive (office) tasks as mail and calendaring. For support, users are on their own. I think that the average user should be able to tackle simple problems with a device. There is also a Yammer group for FAQ."

***MSM03**: "Everyone has the ability to bring an own device and we have classified each device/OS on trustworthy and security. Based on the classification, a user can or can't use certain functionality. If an employee really needs a mobile device for business activities, the device is paid by the organization. The devices are used as supporting devices for office tasks, but also information systems are more and more opened for mobile usage (only by highly trusted devices). There is a support department that helps users with corporate related questions. When the support desk determines that the problem lies with the user's device, the user has to solve the problem itself."*

***MSM04**: "For the 'phone' function we still use Blackberries, for smartphone features users can bring their own iOS device. Every user is allowed to bring one iOS device and use it for basic office functionality like mail, calendar and contacts. Furthermore, iPads are delivered to higher management in order to support them in meetings and presentations. Users can call support for all supported devices, but I honestly think that support is not really needed as these devices are so easy to use and configure."*

***MSM05**: "We have a BYOD environment, iOS and Android are supported and users are only allowed to run behind two software versions of their operating system. Windows phone will be added as soon as all policies can be enforced by our MDM system. Devices are only used for basic supporting tasks as emailing and calendaring. A support desk is available to answer all MDM related questions, when it concerns the device itself the support ends."*

***MSM06**: "We have a BYOD structure for iPads, these can be brought to work and configured for corporate usage. For smartphones, users can order almost any phone they want from our mobile portal. The usage of personal iPads is still a security discussion and it is very possible that this will change in the near future. We use our devices for standard Outlook functionality and we also have a message app to contact other colleagues. Furthermore, an app is developed to let our employees record complains of consumers. For support there is a helpdesk and physical business centers where users can get support."*

***MMS07**: "All devices are delivered by the organization and the 'business' decides whether a user needs a device or not. There are only 4 devices supported (BlackBerry, iPhone, iPad, iPad mini). BYOD is not allowed and in my opinion unmanageable. We use mobile devices for mail, calendar, contacts and document sharing (sharepoint). Primary processes are not supported yet, but this will change in the future. A helpdesk is there to support users in question regarding business usage."*

***MSM08**: "We provide every user with the same device (iPhone) and they are also allowed to bring an own iOS device (iPad). This makes the management of mobile devices much more controllable. Devices are used for basic Outlook functions and chat communication. For support a service desk is available that is trained to support the single delivered device on every problem."*

***MSM10**: "Devices are always provided by our company, but employees are free to choose out of 10 selected devices that are supported. Furthermore, you can use your own device for ActiveSync usage, despite that this is not officially supported. Devices are used for supported tasks (e-mail, agenda and contacts) as well as several primary processes. A service desk is installed to support the 10 selected devices.*

***MSE01**: "During my period as mobile security expert most companies provided the devices and some started with a restricted BYOD program. Devices are only used for supporting processes and there is mostly a support desk in place to answer simple questions and help users to access corporate resources."*

***MSE02**: "More iOS than Android devices that are provided and there are also old windows mobile devices because of legacy software. Windows Phone is not there on a business level. Mostly it is choose your own device (you can choose from a list of devices). With BYOD there are some legal and finance problems. At the moment most companies don't control the ActiveSync protocol which enables any device to connect to their corporate outlook mail/calendar/contacts. Support? Interesting, it is still to be decided who is supporting the devices, mostly an internal department or a 3rd organization."*

***MSE03**: "There is not one model that is used extensively, there are three major models: (1) Bring your own device full throttled, buy anything they want, (2) company decides and buys device for employees and (3) hybrid, company pays certain amount of money and the employee can shop certain phones. Usage is still on supporting processes, not primary processes."*

***MSE04**: "In the past devices were provided by the organization, nowadays more and more BYOD environments exist. This has two reasons, first tax technical mobile: devices are seen as salary and second, supporting and managing mobile devices costs a lot of money. If BYOD is used, it is mostly fully used, which means that all devices that can be managed are allowed. For usage, I see a lot of companies that use mobile devices for supporting business tasks, but also more and more companies that are starting to use mobile devices for their primary process. Support is mostly delivered on the corporate applications, not on the device itself."*

***MSE05**: "BYOD is seen as a trend, but our clients are quitting on BYOD because it is hard to transparently see who is paying for what (contract, internet, device, apps). Most companies choose one device for all employees and some companies have some devices that employees can choose. Company owned devices get full support, where employee owned devices are mostly not supported."*

***MSE09**: "There are two different groups in providing devices, (1) an organization with a lot of external or outworking personal, this group often uses a BYOD/CYOD model and (2) organizations that have mostly internal employees provide the devices themselves. Mobile devices are used for outlook functionality and also more and more for primary processes (mostly outside of the office). Support is mostly available but not for personally owned devices."*

***MSE10**: "Most organizations use a CYOD model or provide the devices to their employees. Devices are mostly used for mail and calendar functionality and sometimes for supportive processes as Sales."*

***MSE11**: "I think a have a bias for this question as we only provide iOS devices that are owned by the company. Still I can say that we see companies that choose one device and companies that let their employees choose a device."*

Tension field between mobile innovation and mobile security

Mobile security managers were asked whether they see a relation between the ability to innovate with mobile solutions and the ability to keep mobile usage secure. They were also asked whether security keeps them from applying mobile solutions in some cases. The mobile security experts were asked if they see a tension field between security & innovation and if their clients postpone mobile solutions because of a lack of security. Figure 21: Innovation vs. Security shows if the interviewees see a tension field between mobile innovation & security.

Conclusion: 80% of the mobile security managers and 71% of the mobile security experts see a direct tension field between mobile security and the possibility to innovate with mobile solutions. The interviewees that did not agree with this statement namely stated that a bad security infrastructure, lack of knowledge on mobile security and more powerful business decision are the reasons for not being able to innovate with mobility and (directly) seeing the tension line between security and innovation. Evaluating the high percentage of positive reactions and well substantiated reasons for not (directly) seeing the tension field concludes that there is a tension field between mobile security and innovation. The organizations and its environment determine how strong and direct this tension field is.

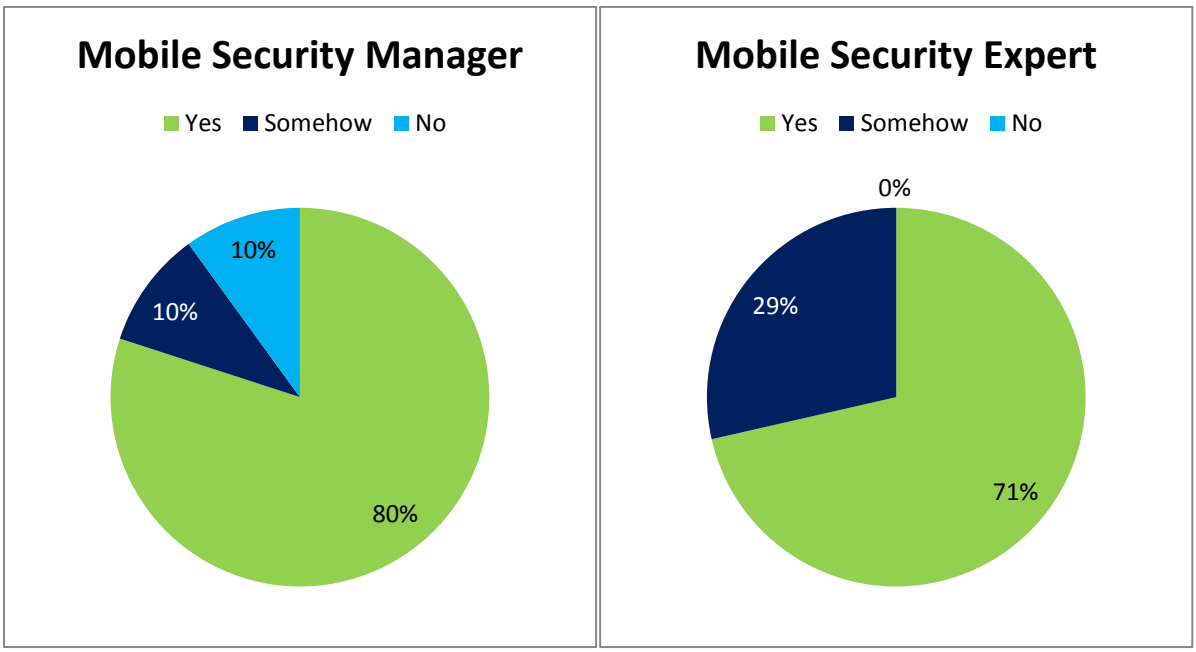


Figure 21: Innovation vs. Security

MSM01: "Yes, innovation is often fast and easy where security like MDM tooling runs behind. Also the fact that app development (mobile solution) is done externally makes it hard to see if security is strong or not. We also see that security is often considered after the implementation, rather than before."

MSM02: "Yes, at least the perception of a tension field. Whether it's always really there, I don't know. A mobile device does not have to be less secure than a personal computer. Mobile security has high priority within organizations and I think that my smartphone is more secure than my desktop. "

MSM03: "This is absolutely the case and this tension field is something that one often wants to use. An example is a mobile application that shows business reports. We defined a policy for this application based on an information classification and trust level of devices. Based on this classification information can or cannot be retrieved."

MSM04: "Yes for sure, you are always overtaken by time. When new operating systems or MDM versions are released security controls change and you have to deal with it. There is a clear tension field between usability and security. People do not want apps in containers when they already have them on their device, you have to be able to convince people on the need for security controls."

MSM05: "Reasonable, brainstorming on innovation or functionality is done without taking security in mind. Then the idea will be evaluated on risks and security control possibilities. Mostly, there are

enough controls to allow the innovation but sometimes innovations are indeed cancelled due lacking security measures."

***MSM06**: "Yes for sure, some mobile solutions can't be done because of security reasons. Sometimes it is also the question if you want a certain person to deal with certain information on a mobile device or if you want to have certain information on a mobile device in the first place. Sometimes innovation can be done with technical controls but then the user awareness lacks and we still decide to not innovate due security reasons."*

***MSM07**: "Yes absolutely, it's a trade-off between usability and security. Often business question arise to innovate but are cancelled due to security reasons. That is also the reason why we still not fully support primary processes."*

***MSM08**: "Yes it does, it limits mobile innovation. Our supervisory authority also demands security controls that limit innovation. Mostly innovations are delayed and not directly stopped, than controls are installed."*

***MSM09**: ''Yes, we are waiting for MDM solutions to get mature before we want to further innovate with mobility on primary processes."*

***MSM10**: "Yes, for sure. Security controls always compromise usability and the possibility to truewely innovate. For example: employees would like to access the intranet on their mobile device, this is not allowed due to security reasons."*

***MSE02**: "Yes it was a problem but new technologies are able to cope with these problems, with applications wrapping etc. You can now encrypt, VPN and wrap existing apps easily.*

***MSE03**: "Yes, I totally agree. If you take it to the extreme, if security wasn't an issue employees could do anything they want. From that perspective security is the big roadblock. It can also be about management but that also leads back to security. The only roadblock to innovation is security!"*

***MSE04**: "Organizations are afraid of the unknown, personal computers are known if you talk about security and vulnerabilities, and mobile devices are still new. Mobile security has high priority and I think there is a tension field, and that is why organizations spent so much time on security and risk analysis before they innovate with mobility."*

***MSE05**: "Yes for enterprise organizations this is certainly true. For smaller organizations, this is less of an issue as they are more concerned about cost and added value of mobile solutions."*

***MSE09**: "I do think a tension field exists and that this makes security more advanced. I don't think that security often keeps companies from innovating; it is more that it delays innovation. Security is also often used as an excuse for not innovating."*

***MSE10**: "Yes, it also often depends on the vision of the CISO. A CISO that is not aware of mobile technology and threats is often afraid of innovating, because he is not able to assess the impact. Security will always influence innovation but there are good measures to make mobile innovation possible."*

***MSE11**: "More or less, if you have a good security model and a modern infrastructure mobile innovation should not be a problem. Often these things are not in place and security becomes a opponent to innovation."*

Usage monitoring

The MSM interviewees were asked whether they monitor which devices, OS versions, apps and data is used within their enterprise environment. Furthermore, they are asked why they monitor or why they do not. The mobile experts are asked the same questions on how and why their clients are monitoring devices, OS versions, apps and data. Figure 22: Monitoring of device, OS, app & data provides an overview on how the interviewee's responded to this question.

Conclusion: The four defined groups in Figure 22: Monitoring of device, OS, app & data clearly identify the four different statements of managers and experts. The biggest group monitors devices and OS versions mostly by using a MDM system. The other interviewees, not using monitoring often state that they don't see the added value of monitoring or that privacy and legislation keep them from monitoring mobile devices. The most important conclusion is that monitoring is never used in a more advanced way than device and OS monitoring. Tracking of app usage and data usage is never done, due to privacy reasons as well as technical and organizations capabilities.

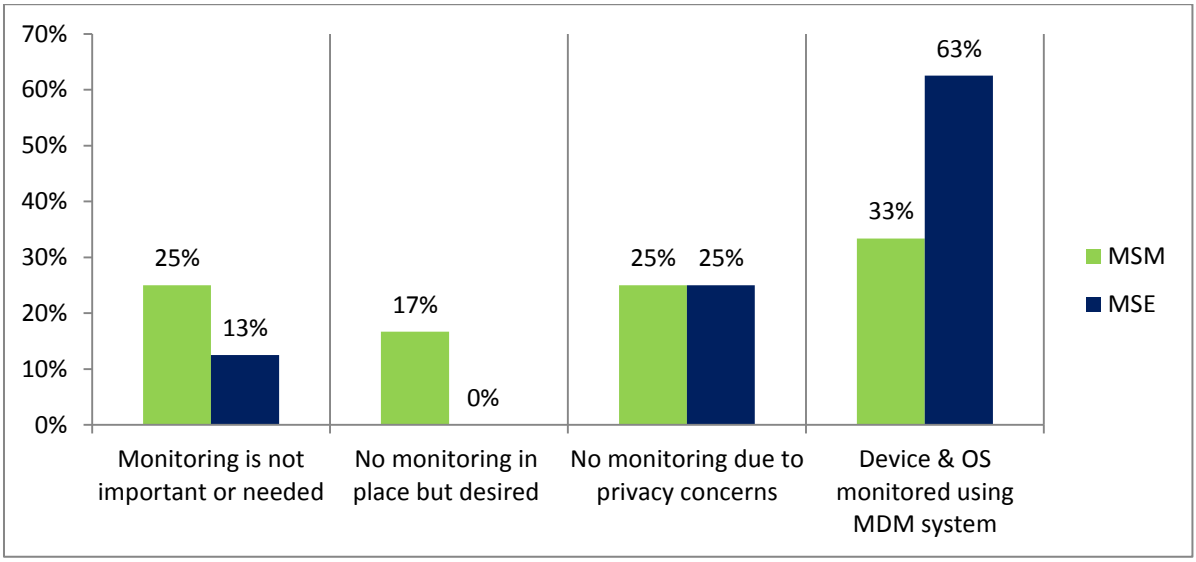


Figure 22: Monitoring of device, OS, app & data

MSM01: "Currently there is no insight in how devices, apps and data are used. In the near future we will use a MDM system to monitor the status of devices. I don't worry much about iOS devices, but Android and Windows is a different story. We need to white or black list applications and be able to monitor this policy."

MSM02: "Our MDM system is only used to monitor how many devices are around. As the MDM system enforces all policy rules I don't see the added value of monitoring devices. Furthermore, we see different privacy issues in monitoring devices. As our employees are travelling all over the world, we also have to cope with privacy and regulations in foreign countries."

MSM03: "We do measure which devices & OS versions are used and we can also see which apps are installed. Installed apps are already on the sensitive boundaries of user privacy. Furthermore, devices are managed correctly and we don't see any need to monitor everything."

MSM04: "Our MDM system is used to monitor which device users are using, which OS they are running and which apps are installed. Users are only allowed to bring 1 privately owned device. We also use the MDM system to control this policy."

***MSM05**: "We don't monitor anything and I also can't find any reason why we should do that. We enforce all needed policies by our MDM system, so there is no need to monitor."*

***MSM06**: "As far as I know we don't monitor anything actively. However, we are capable of monitoring almost anything. Due to privacy regulation and legal issues we are not allowed to monitor anything."*

***MSM07**: "Our MDM system monitors the used devices and the operating system that is running on it in order to act when users are not updating their mobile device fast enough. Furthermore, we can scan all internal network traffic via a proxy. The data that is used outside of the corporate environment cannot be monitored."*

***MSM08**: "In our standard environment there is no monitoring in place. However, we are currently doing pilots with MDM systems that also contain monitoring functionality."*

***MSM09**: "We don't monitor any specific things. We do detect when people are using extreme amounts of data and ask them to explain why this is occurring."*

***MSM10**: "ActiveSync is used to monitor which devices and OS versions are used by which people. When a MDM system is in place we will make more usage of monitoring functionality."*

***MSE02**: "Organizations often monitor devices and app uses via their MDM system. The console provides information on device type, OS version and installed apps. With Android, you can enforce that apps are blacklisted, with iOS this is not possible as the user remains all rights to run any appstore approved app."*

***MSE03**: "Depends on what the purpose is and what the model (BYOD or not) is. When mobile devices are not allowed, you first need to know why and if employees are using devices. If the company provides the devices, you should monitor the devices with a MDM tool. With BYOD it depends on regulation and privacy issues within the country."*

***MSE04**: "Monitoring is not needed and often not wished due to privacy issues. If you correctly enforce which devices, OS, and apps are allowed you don't have to monitor anything. If you use an enterprise sandbox environment to open enterprise data, it is also not needed to further monitor data."*

***MSE05**: "Mostly MDM systems are used to monitor which devices and corresponding OS versions are used. Applications are always a privacy discussion point and mostly not monitored. Previously, non-trusted applications like Dropbox were blocked on policy level. Nowadays it is more important to provide an enterprise alternative for applications as Dropbox. Data monitoring is even more privacy sensitive and never monitored. Data and application containerization is more and more enrolled within enterprise organization. Furthermore, awareness programs and user trainings remain important for information security as it is always possible to send corporate data to a private environment".*

***MSE09**: "Monitoring is often very minimal or not installed. I think that a lot of organizations can improve on monitoring in general. Still, privacy and compliance issues are also hard to deal with when monitoring mobile devices."*

***MSE10**: "Mature organizations often use MDM to monitor devices and the OS of devices. Usage of devices and/or apps if often not monitored due to privacy and compliance issues."*

***MSE11**: "Organizations mostly don't have a MDM solution and do not monitor anything. Organizations that do have such a solution only monitor devices and the operating system."*

Mobile threats

Mobile Security Managers are asked what they consider the most important threats, what threats get too less attention, how threats are identified and if threats already became reality. The mobile experts are asked the same questions to understand what they consider the most important and underestimated threats. Figure 23: Mobile threat classification by MSM & MSE shows an overview on what threats are considered most serious by the interviewed managers and experts. The threat that is considered most important is valued with three points, the second with two points and the third with one point. If an interviewee provides more than three important threats the less important are all valued with one point. The percentages in Figure 23: Mobile threat classification by MSM & MSE are based on the total given points per category by the MSM and the MSE.

Conclusion: Data loss is by far the most important threat identified by managers as well as experts. Also leaking client data, which is directly related, is identified by several managers. Managers also identify a greater risk to damage their company image by not using mobile in an appropriate way. Some experienced mobile security experts identify more advanced threats as 'mobile as a pivot point', 'blurred lines between private & business usage' and 'BYOD usage by unregistered users'. Important to conclude is that data loss is the threat that is identified as most important and that there are more advanced threats that certainly need to be considered and are not always on the scope of organizations.

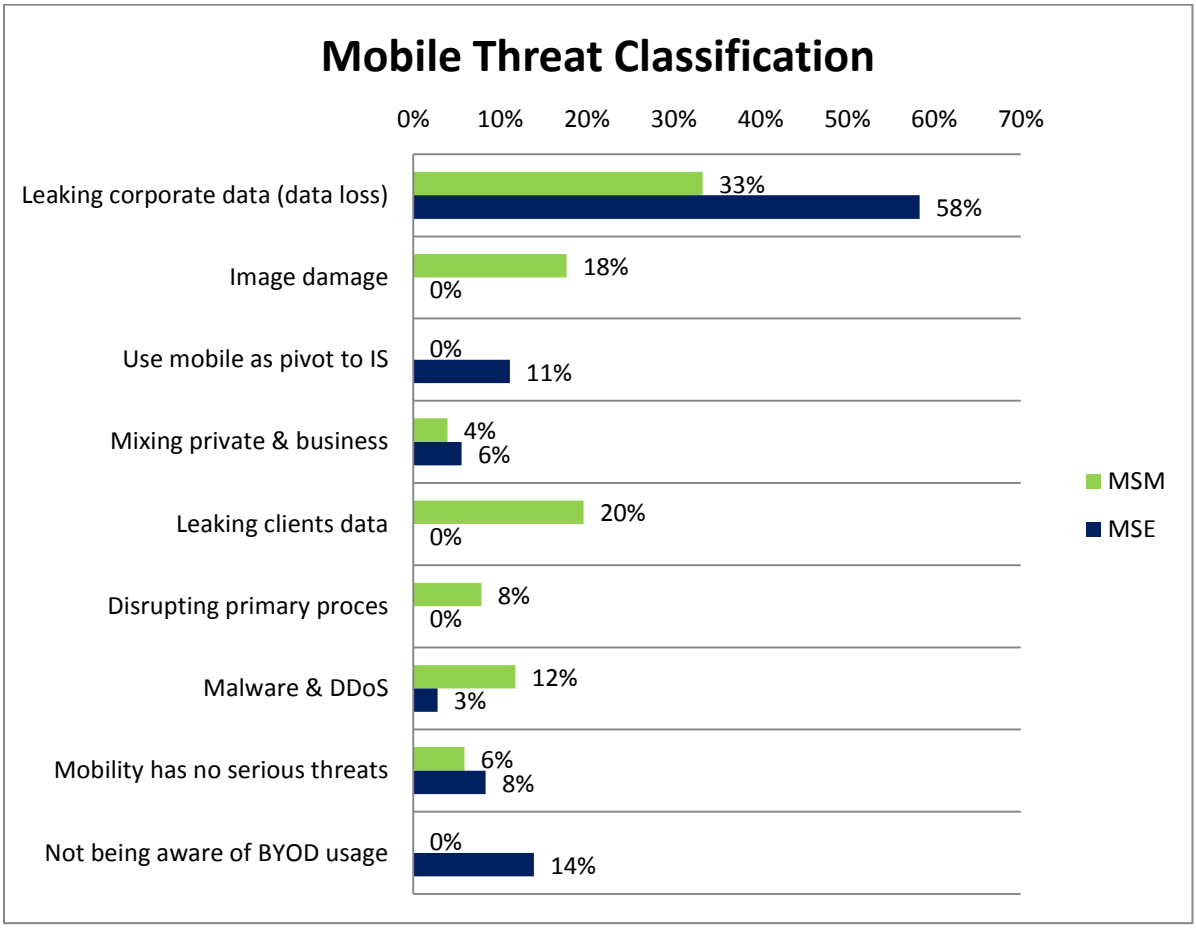


Figure 23: Mobile threat classification by MSM & MSE

MSM01: "As we are mostly working with sensitive information of clients, our trusted image is most important and thus our main concern. Combined with the leakage of sensitive data from our clients (which results in a damaged image) these are the two most important threats. A third threat is the disruption of our primary processes as we are using mobile devices in primary processes. When these devices will be compromised our primary process is disrupted, which will cost direct income. I think all threats get enough attention and our time is divided efficient. The identification of threats is done through external specialists that provide a report when functionality is changed. Our most feared threats haven't become reality yet."

MSM02: "Leaking strategic information is the most important threat, when information leaves the corporate sandbox we completely lose control of the data. The second important threat is mixing private activities with business activities and vice versa. To give an example, when an enterprise mail is answered with a private G-mail account, the attachment will be indexed and then we lose control of the attached information. An upcoming threat is malware, compared to the other threats less important, but that will likely change in the future. I think that there aren't threats that get too less attention, but that doesn't mean that there are no challenges. Especially dealing with laws and regulation on privacy & encryption in different countries remains challenging. For the identification of threats we use the IRAM (Information Risk Assessment Methodology). We conduct this analysis when new functionality is introduced and with a standard interval of three years."

*MSM03: "Leaking business information is the only threat I see and I don't think that there are any threats that get too less attention. There is a separate team that conducts the risk assessment for mobile usage, I'm not familiar with their exact approach but I know that they use an impact * likelihood analysis. As far as I know, there are no cases where business information is leaked through a mobile devices."*

MSM04: "In the first place leaking sensitive information, secondly the damage of our corporate image that can be through the leakage of information or by other means like losing a device."

MSM05: "Emerging malware is the biggest threat, targeted as well as opportunistic. The leakage of sensitive information is not important anymore as controls are already mature. I don't think that there are threats that get too less attention at the moment. When we start using mobile devices in primary processes this will change and new threats will arise."

MSM06: "Leaking client information and leaking our own strategic information by losing a device or being hacked from the outside."

MSM07: "Data loss in the first place, also damaging our corporate image. We can't afford that client's data on a lawsuit becomes publicly. DDoS attacks are also a threat as we are a target that is often attacked, but this is much less important."

MSM08: "The most important threat is reputation damage. Secondly , data loss of our own data but also financial data from our clients."

MSM09: "I don't think that there are any serious threats for mobile that are different from already existing threats."

MSM10: "Disruption of our primary process is the most important one, at the moment there are only few mobile applications that can really disrupt our primary process but this will change in the near future. Also data confidentiality, thus data loss is an important threat."

***MSE01**: "Leaking sensitive information remains the most important threat for organizations. Other threats are there but are subordinate.*

***MSE02**: "I don't think that mobile threats really exists as long as you have the right controls in place. Data is always encrypted and devices are managed, that is enough. It's more that companies trying to tick the compliance boxes for legal and regulations than that they are really concerned about a threat. When known threats are exposed, you often see that companies start asking for new solutions in order to control the exposed threat."*

***MSE03**: "Leakage of corporate information (data loss), malware isn't a big issue in Europe and the USA, in China it is. Important one is to use the mobile device as a pivot point to get in the corporate data/resources. Business process disruption is not yet an issue as companies are not using there devices primary. It is always on top of the laptop/desktop. Financially being robbed is also not really an issue as European countries always have two-way authentication. Use the mobile device as a pivot point to get in the corporate data/ resources is a threat that is mostly not considered by companies. Furthermore, having credentials on the mobile device for Facebook or other accounts is a big threat as it is very likely that one of your passwords can be used (together with your corporate email account) to log in to your corporate network. I don't think that attacks are that big as they are written by many people. There are threats on mobile level but they are not that serious in my opinion. Compared to web applications there is one big difference, everybody on the planet has direct access to the web applications and is able to attack it. This is not the case with mobile devices. So it is less an issue than webapps for instance. Nevertheless, it is still a challange that needs to be addressed."*

***MSE04**: "Business critical information that is available to the wrong persons is the biggest and probably the only threat to organizations."*

***MSE05**: "In the first place the leakage of corporate information when devices are lost or stolen and not properly secured. The second threat is on governance level, to give an example: organizations are often not aware of the amount of exchange accounts that are linked to unknown private devices. Threats are identified by conducting interviews and using experience. There is a clear dichotomy when talking about threat awareness in organizations. Large enterprises are very aware of the possible threats with mobility in contrast to smaller organizations, which are more concentrated on the added value and usability. Threats that become reality are only found in the form of lost or stolen devices. Companies mostly start thinking of mobile security when a device form a person on board level gets compromised."*

***MSE09**: "Data loss remains the most important threat. Data travels around the world on mobile devices, which makes it very hard to manage for security officers. Email is often highly underestimated but is a very serious problem as data (attachments) is mostly not classified. Furthermore, I see a threat when a mobile device is used as a pivot point to access enterprise information sources."*

***MSE10**: "Data loss is the most important threat, but also the blurred line between private and business uses is a threat in my opinion. A third one for the organizations is to get troubles with privacy issues on employee owned devices."*

***MSE11**: "The most important one is data loss by losing a device and not protecting the data. Secondly the fragmentation of the Android operating system is also a big threat for some organizations. There are so many versions and the software update adoption process is often very slow."*

Risk assessment & acceptance

Mobile Security Managers are asked if and how they calculate the risks that originate from mobile usage. Furthermore the frequency or trigger to evaluate or re-evaluate these risks is identified, as well as the process of accepting mobile risks. The Mobile Security Experts are asked how a risk analysis should be conducted and in what frequency mobile risks should be re-evaluated. Figure 24: Risk Assessment Approach & Assessment interval shows which risk assessment methods are used by the interviewed managers and experts and shows when assessment are repeated.

Conclusion: Most important to conclude is that organizations have a risk assessment process in place. Most organizations use an accepted industry standard method for information systems or just determine the likelihood and impact of a risk. There is also a group of organizations that outsource this process due to a lack of knowledge or to prevent a tunnel vision on possible threats and risks. Risk assessments are always conducted when new functionality is installed and some organizations complement to the functionality trigger and also conduct risk assessments on a determined time interval.

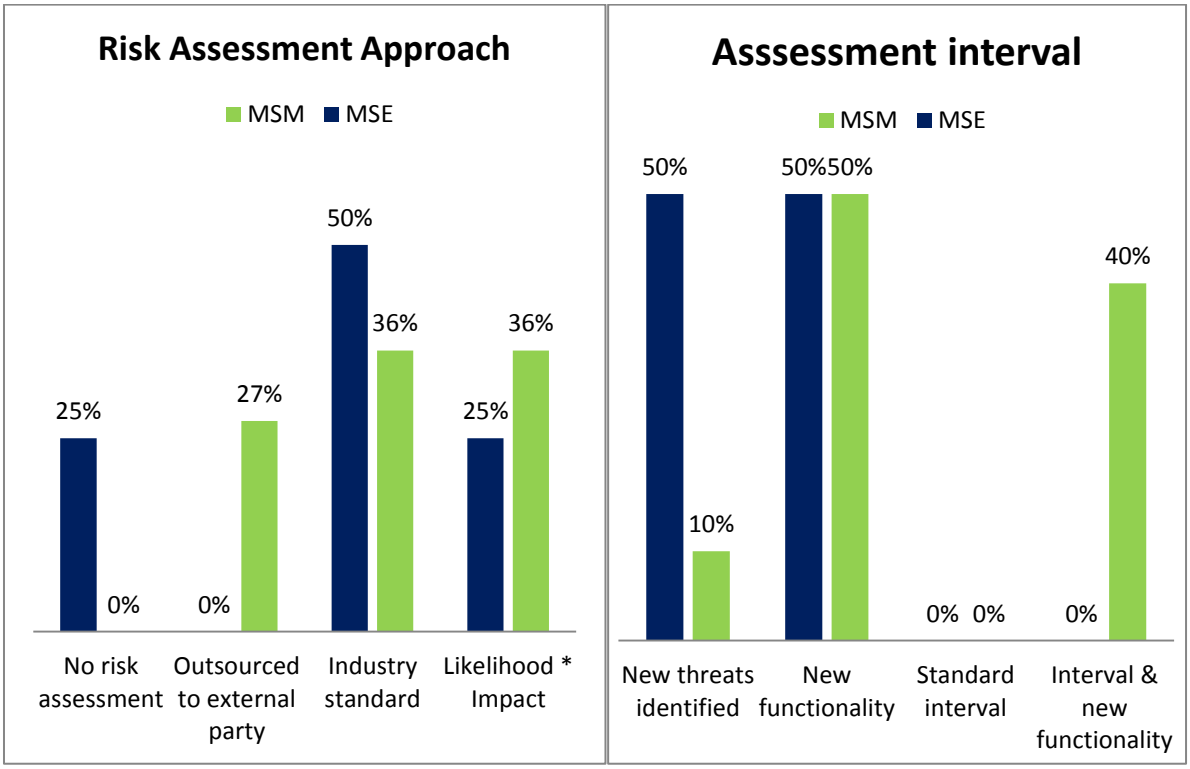


Figure 24: Risk Assessment Approach & Assessment interval

MSM01: "Risk analyses are executed by external parties like Deloitte. The analyses are mostly based on likelihood and impact. When the risk report with residual risks is delivered, it will be discussed and formally accepted or denied at the management team of our organization. Risk assessments are always conducted when new functionality is introduced. There is no standard interval for a re-assessment."

MSM02 "We use a semi-quantitative tool called IRAM to assess mobile risks. IRAM consists of a Threat Vulnerability Analysis and a Business Impact Analysis. Risks are not measured in exact amounts of money but are classified in categories of amounts. When the assessment is concluded, each risk is evaluated by the risk counsel and then formally accepted or denied. Risk assessments are always conducted when new functionality or changes are made, but also in a standard interval of 5 years."

***MSM03**: "Risk assessments are executed by a separate department. We support this department in identifying existing threats and implemented controls. I'm not aware of the exact method that is used for these assessments. If and who is responsible for accepting or denying risks is a very good question, which triggers me to find out how this is regulated. When a risk encounters the loss of sensitive information, not only the security officer should accept the risk but also the business owner of the information."*

***MSM04**: "Our risk management department determined a risk model with 36 levels of risk. Each level has its own consequences and decides on what level acceptance should be decided. The analysis is done using a likelihood * impact method. Risk analyses are executed when new functionality is introduced or when new threats are identified."*

***MSM05**: "We use a likelihood times impact analyses to determine mobile risks. An assessment is always done when new functionality or changes are introduced. Risks are formally accepted by the business owner, the risk magnitude decides on which level it needs to be accepted. Furthermore, each year a list of risk priorities is made to identify which systems should be re-evaluated.*

***MSM06**: "A BIA (Business Impact Analysis) and risk analysis is executed when new products or services are introduced. A risk framework is used to decide when an assessment needs to be executed and who is responsible for accepting the risk."*

***MSM07**: "Security is a standard agenda point with every change or new functionality. The risk analysis is part of this agenda point and is always executed by an external party like Deloitte. The steering committee decides whether a risk is accepted or not."*

***MSM08**: "A BIA is used based on the CIA (Confidentiality, Integrity and Availability) to assess mobile risks. Risks are re-evaluated when new functionality is installed and also bases on a standard interval that depends on the impact of the risk."*

***MSM10**: "Quantitative analyses are used to perform a Business Impact Analysis. Risks assessments are conducted when new functionality is installed and on an annual recurrence."*

***MSE01**: "Traditional 'likelihood * impact' methodologies are also suitable for mobile risk assessments. NIST provides some guidelines that are specially used for mobility and it is wise to consider these.*

***MSE03**: "I don't have a good view on which method is best to use for a mobile risk assessment. The frequency of assessments should not be based on a standard time frequency but based on new functionality like new devices, operating systems, MDM versions or corporate apps.*

***MSE05**: "We mostly use an ad-hoc analysis where we explain our clients what the impact of certain risks can be, but we don't use any formal risk assessment method. Risks are only re-evaluated when a client asks for it. We don't see any clients doing periodical re-evaluations."*

***MSE11**: "Traditional risk assessment methods should also be applicable for mobile. A BIA analyses should also be conducted as part of the risk assessment.*

Controls & MDM

Mobile Security Managers are asked if and how they link controls to risks, threats or vulnerabilities. They are also asked if they are using a MDM system to enforce controls and how this system is solving their security and governance problems. Figure 25: Control reference & MDM influence shows if and how managers link their mitigating controls to risks or vulnerabilities. Furthermore, the figure shows to what extend managers find their MDM system capable of enforcing their determined mobile security policy.

Conclusion: The interviewed mobile security managers were quite diverse on how mitigating controls were related to earlier identified vulnerabilities or risks. Some of the managers didn't link controls back to their source at all, where most managers stated that the controls were somehow related to identified vulnerabilities or risks. The managers that did use a MDM system to enforce controls stated that their MDM system was able to enforce technical policies, but also that a MDM system is not capable of solving the complete mobile security issue.

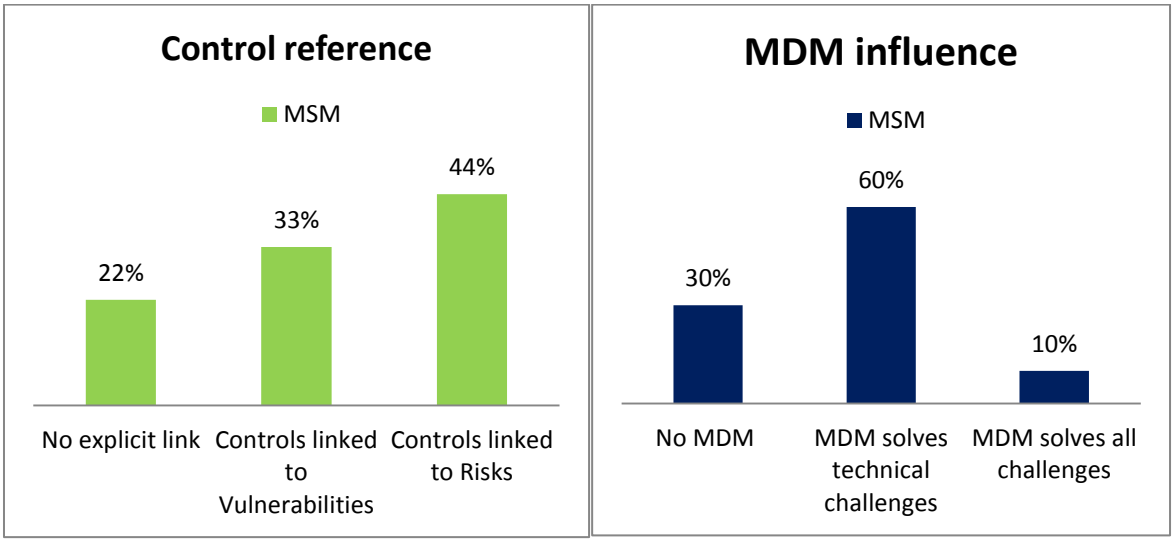


Figure 25: Control reference & MDM influence

MSM01: "Controls are linked to determined risks, when new risks are identified controls are linked to see if a risk is covered. Currently we don't have a MDM system in place, but we are working on it. The MDM system will first focus on Android devices as they bring the biggest risk.

MSM02: "By following the IRAM methodology, controls are linked to the vulnerabilities that they mitigate. A MDM system is used to manage all our mobile devices. The system solves our security and governance challenges for the biggest part. Malware problems, remote management and encrypted connections to other systems are all managed by the MDM system. However, due to usability reasons it is still possible to bring corporate data out of the sandbox into private apps. Also, user awareness en responsible usage cannot be solved with a MDM system."

MSM03: "Mitigating controls are linked to vulnerabilities. Our MDM system solves most of the technical problems but lacks in functionality when other systems need to be securely linked to the mobile device. Furthermore, user and process problems cannot be solved using a MDM system."

MSM04: "The mitigating controls are always linked to the identified vulnerabilities. These controls are mostly enforced by our MDM system, MobileIron. This MDM system has great features but we still don't use them all. Due to license cost only limited functions are used at the moment. The system fulfills all our wishes and we are still looking to implement new features that the system standardly offers."

MSM05: "Controls are always linked to risks. MDM solves the majority of technical problems, but there always remains a part you can't control. Furthermore, we always depend on how the user acts regarding its mobile device."

MSM06: "Controls are related to risks. On a regularly basis controls are checked if they still cover the identified risks that are changing due to a moving mobile environment. We do use a MDM system to enforce our defined policies and the system covers all desired technical policy enforcements."

MSM07: "Risks are identified and the controls are later linked to the defined risks. The requirements that we ask on security are all covered by our MDM system. We are still looking to implement new features that our MDM system offers. Mobility has gone really fast and we didn't have a complete security proof policy for mobility, which is why the system is used as a basis for our policy."

MSM08: "There is no explicit link between controls and risks. Controls are installed during the process but are not backwards related. We don't have a MDM system in place yet, but we are conducting test pilots with MDM solutions. MDM's should be capable of enforcing all technical policies, legal aspects are also still challenging when using a MDM system.

MSM10: "Controls are not directly related as controls are mostly installed for multiple risks or threats. Every business unit can use its own MDM solution, but most are still testing with MDM systems.

MSM09: "We don't have any MDM in place at the moment. The problem with MDM systems is that they always require additional software on a device. We don't want to be depending on this extra MDM software and constantly waiting for an update when the operating system of a device is updated or a new operating system is introduced. When MDM systems become more mature and operating system independent we will start using them and use the full potential of mobility."

BYOD impact

The Mobile Security Managers as well as the Mobile Security Experts are asked how mobile security changes when a BYOD program is introduced. For some managers this is easy to answer as they are currently having or enrolling a BYOD program, for others it can be hard to imagine that their organization will introduce a BYOD program.

Conclusion: Most managers as well as experts start with explaining that BYOD will likely never happen to their organization or to organizations that are advised. But if higher management decides and BYOD has to be managed, different actions are named. Most of the actions can be categorized into four groups, (1) 'Advanced MDM', using a MDM system to enforce complete control of the mobile device, (2) 'Follow data', focus on the security of enterprise data that is on consumer devices, (3) 'User awareness', train and educate users on how to deal with enterprise data on a private device and (4) 'Privacy and legislation', make sure that all enforced policies are within the law of privacy.

MSM01: "Introducing a BYOD program is not going to happen in our organization as mobile devices need to be very specific configured in order to support our primary process. When we should introduce a BYOD program, the most important measure is ensuring an encrypted and safe connection to our source systems. Protecting sensitive information of our clients becomes even more challenging. I also think that managing BYOD is two-fold, the organization as well as the user needs to manage the device."

MSM02: "On a governance level it is important to determine who is responsible for certain risks and what the legal & compliance issues are. Also device lifecycle management is important as the user

decides which device is used. MDM becomes even more important and needs to be used to enforce processes as well as technical measures."

***MSM04**: "I don't think it will happen for us in the near future but when it does, we firstly have to identify whether our MDM solution is still satisfying. Furthermore, apps need to be containerized, device registration should be mandatory and user policies should be tightened."*

***MSM05**: "BYOD with supporting processes as e-mail is manageable. This will change when primary processes are taken mobile. When this will happen, BYOD becomes a real challenge for security and it becomes extremely hard to protect source systems."*

***MSM06**: "Due to economic reasons (we can deliver mobile devices really cheap) we will probably never introduce a BYOD program. If you need to enroll a BYOD program, enforcing your enterprise policy is the most important and first thing to do."*

***MSM07**: "Focus on information security, make sure that the data is secure and concentrate less on the device. Furthermore, users need to be educated and the legal department should dive into privacy regulations."*

***MSM08**: "When enabling BYOD three groups of devices should be made, (1) trusted devices, which are owned and managed by the company, (2) compliant devices, which don't belong to the company but do satisfy a standard set of security controls and can be managed by the organization's MDM and (3) untrusted devices that are not trusted and cannot be used for accessing enterprise resources. The security policies should be enforced by MDM or ActiveSync. Furthermore, legal aspects should be considered and explained to employees."*

***MSM10**: "The line between business and private disappears with BYOD. It is important to focus on data protection, when data is on the device it should be managed by the organization. MDM or Unified Access Gateway can be used to manage enterprise data."*

***MSE02**: "Deciding which devices and which policies you need, and decide on a legal basis what you can enforce on a personal device. Also which users are going to use devices and how are they going to use devices. For instance, in Germany they have very strict laws, when corporate information is on a device the device owner becomes owner of the information."*

***MSE03**: "Think years ahead on functionality and security before allowing devices. If a device becomes unsupported after a few years you shouldn't allow them. Make sure that the security policies are able to execute otherwise you lose support from employees. Then look for the tools that can enforce your policies & security demand and then the last step is to allow a selection of devices and OS's."*

***MSE04**: "Important with BYOD but often forgotten is the process of activating a device. This process is very important and can go very wrong. There are self-supporting tools that can make this process very rigorous and easy for the end-user. "*

***MSE05**: "I think that the following steps should be encountered when starting a BYOD program:"*

1. *Determine mobile strategy*
2. *Determine mobile policy*
3. *Device selection*
4. *MDM selection*
5. *Implementation & training*
6. *Awareness program*

***MSE06**: "The most important activity is deciding which operating systems and devices are allowed and what vulnerabilities these devices encounter."*

***MSE10**: "I honestly think that full BYOD is not an option. You just can secure all devices and operating systems that are around."*

Artifact concept

Based on the theoretical study and semi-structured interviews with Deloitte experts, a concept of the high-level M-RAM artifact was created. The concept was introduced during expert interviews in order to provide feedback and let experts think about how a mobile risk management method should look like. The concept artifact was incrementally changed using the feedback gained in expert interviews. Experts that are not included in the quote list or figures did not find they were eligible to comment on the M-RAM concept or did not have any comments on the M-RAM concept. The logic behind these statements and the M-RAM artifact will be further explained in section 5 Artifact Components. This subject does not include a conclusion, as the proposed attention areas and involved entities are opinions of the different experts, and do not answer a specific research question.

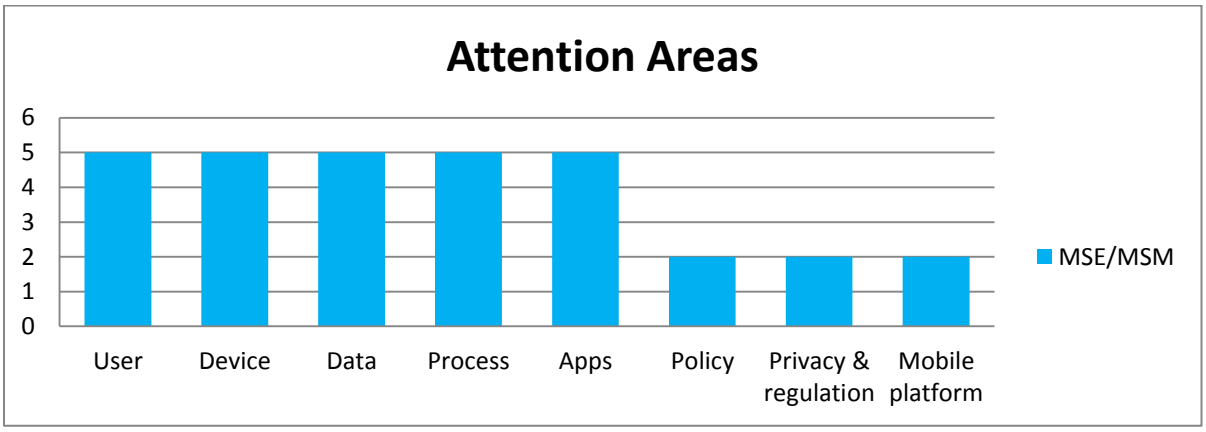


Figure 26: Expert Attention Areas

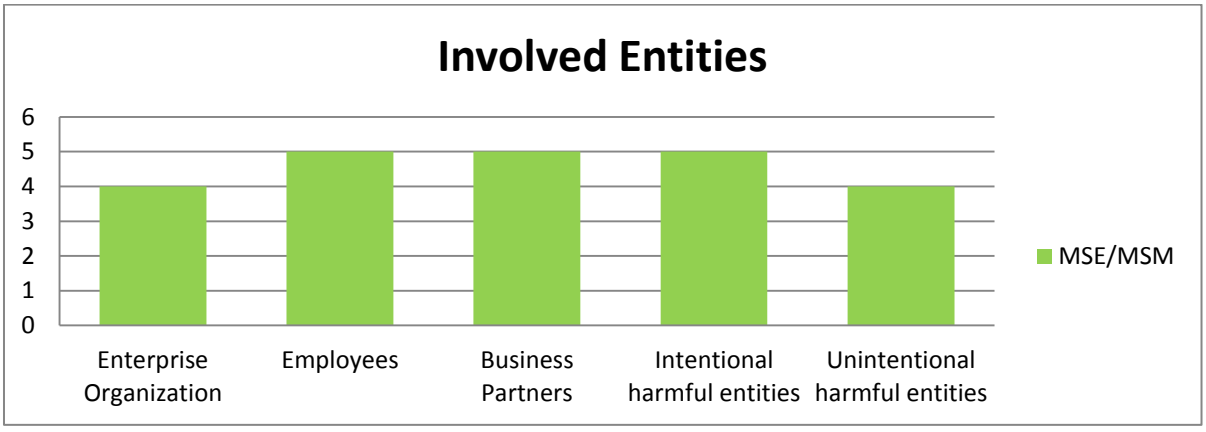


Figure 27: Expert Involved Entities

***MSM02** "I think that there aren't threats that get too less attention, but that doesn't mean that there are no challenges. Especially dealing with laws and regulation on privacy & encryption in different countries remains challenging".*

***MSM05** "The attention area 'governance' is too vague, it is better explained as policies, compliance or other things you mean with governance."*

***MSM10**: "The involved entity 'Business Partners' should also include suppliers and customers, this should be explained elaborately. I think that threat tolerance should also be part of the 'Identify events, threats and vulnerabilities' step."*

***MSE01**: "The method seems logic to me, the process is relatively standard compared to default risk assessment processes, which is logical. The entity 'environment' is not clear. I would split it in 'partners & clients' and 'hackers'. The attention areas are understandable but I would add applications and I would change governance into policy."*

***MSE02**: "Organizations need to use a method like this one; I think the process, entities and attention areas are very clear. An important addition would be the entity that is unintentionally harmful to the organization. The biggest example is a kid playing with a mobile device and unintentionally exposing sensitive information. Furthermore, adding 'apps' as an attention area is needed to be complete."*

***MSE07**: "To be honest I don't get the difference between the enterprise organization and employees. What other entity is in enterprise organization besides its employees if you excluded business partners? With the assessment process, I'd say "Information assets" instead of "mobile assets", mobile security is part of information security. By assuring the security of mobile devices you want to achieve overall security of the whole environment. You should involve every information assets which can be accessible from mobile devices - e.g. intranet pages or internal web application should be part of the risk assessment and it is not considered as just "mobile assets". For the attention areas I would add 'applications' and 'mobile platform', if you do a risk assessment you also have to look at the platform that is used to provide and manage mobility. Furthermore, I would change attention area 'process' to 'control processes' so that it is clear that it is about controlling the mobility usage process."*

***MSE09**: "As with cyber security, traditional risk assessment models are not always working anymore. Models are focused on letting the business accept residual risks. But the question nowadays is whether the business is really capable of assessing these risks as hackers and cyber criminals become very sophisticated. Cyber criminals are mostly looking to combine very small vulnerabilities with very low likelihood to attack an organization; these vulnerabilities are mostly accepted as residual by the business. This concludes in a mismatch between the capabilities of criminals and the business. I think that we should not focus on risks but on threats and forget about likelihood, when vulnerability exists it will be used against you, no matter how small the likelihood is. The attention area 'mobile platform' seems the same as 'mobile devices' so this should be renamed. 'Control processes' is very good and you should also focus on the processes at the front of mobile usage. Furthermore, I would split application and data as the controls are very different. Maybe you should also look at the consecution of the attention area and if you give that a meaning."*

5 Artifact Components

The components of the envisioned artifact will be introduced in this chapter following step 6, 7, 8 and 9 of the research process. Section 5.1 Artifact Introduction explains why the artifact is designed. Furthermore, section 5.1 explains which components are parts of the artifact and what the relation is between the different components. Section 5.2 Entities, 5.3 Risk Assessment Process and 5.4 Attention Areas elaborately explain the key components of the M-RAM artifact.

5.1 Artifact Introduction

"Before designing and deploying mobile device solutions, organizations should develop system threat models for the mobile devices and the resources that are accessed through the mobile devices. Threat modeling involves identifying resources of interest and the feasible threats, vulnerabilities, and security controls related to these resources, then quantifying the likelihood of successful attacks and their impacts, and finally analyzing this information to determine where security controls need to be improved or added. (NIST, 2013)"

The problem statement of this research *"Enterprise organizations are struggling in governing their mobility usage and there is no existing approach that delivers guidance in assessing and managing risks that originate from mobility"* defines that organizations having trouble to control the risks that originate from mobility. Interview results validate this as organizations are using existing information system assessments, outsourcing mobile risk management or do not have any risk management process in place for mobility. The development of a mobile specific artifact is needed in order to solve this problem. The artifact should provide organizations the means to identify what risks they take with their current mobility usage, what controls they have to mitigate these risks and how big the residual risk is.

Different artifact forms can be imagined to support organizations in the itemized problem. A 'framework' artifact would identify attention areas so that one knows where to identify mobile threats, vulnerabilities and risks, but would lack in providing an approach to actually do the identification. A 'process' artifact would explain which steps are needed in order to execute a mobile risk assessment, but would lack the attention areas where mobile threats, vulnerabilities and risks need to be identified. Combining these artifact forms using a 'method' artifact enables an organization to perform a solid mobile risk assessment. By following a predefined approach to each process step, being aware of the scope of mobile security and feature detailed mobile risk attention areas a 'method' artifact suites the requirements of this problem solution.

The M-RAM 'method' artifact will be based on three core components, (1) the involved entities, (2) the risk assessment process and (3) the attention areas. The first component determines which entities are involved in the field of enterprise mobility, what the role of each entity is, how they can affect risks related to mobility and how they are involved during the risk assessment. The second component is the core of the method as it provides the mobile risk assessment process and an approach to execute each process step. The last step provides a set of attention areas that should be taken into account during the risk assessment. Each attention area will consist of vulnerability guidelines and control opportunities. The following sections explain each component in detail and the next chapter explains how the components are combined in the M-RAM artifact.

5.2 Entities

This section provides an answer to the stated *SRQ3: Which entities are involved with enterprise mobility and how are these involved?* Enterprise mobility involves different entities and actors, internally as well externally. Identifying these entities is important as every involved entity can influence possible risks. The internal parties are easy to identify as these are all part of the enterprise organization that is assessed. In contrast to the internal entities, the external entities are much

harder to identify, as it can be any entity that can possibly become a threat to the enterprise organization.

Internal entities can be summarized as the management of the organization, the employees and the IT department. The management of the organization is responsible for the vision/strategy on enterprise mobility. Furthermore, the management of the organization is also the sponsor of all enterprise mobility initiatives. The IT department can be seen as part of the organization as it executes the vision/strategy of the management organization. However, the IT department can also be seen as a different entity, as it is responsible for controlling and governing a secure mobile environment. The employees are the users of enterprise mobility and therefor an important entity. The interpretation of enterprise mobility can rigorously change how employees are involved with enterprise mobility. Employees of a fully BYOD enabled company carry a different role in enterprise mobility, compared to employees that use a fully managed, company owned device.

As mentioned before, external entities are far more complex to identify and categorize. The most important high level entity is the group of entities that intentionally or unintentionally trying to harm the organization. This group is very broad and needs to be further explained as entities can vary from children that unintentionally sent sensitive information from a corporate tablet to organized criminals that try to use mobile malware attacks to gain corporate credentials. Furthermore, entities that work together with an organization and access enterprise systems (through mobile devices) is another group of entities that need to be considered. These entities can vary from supply chain partners that are part of a company's process to external consultants that are hired to work for the assessed organization and are temporarily using and accessing enterprise resources.

The identification, grouping and naming of entities is initiated by interviewing internal experts. The output of these internal interviews provided a basic understanding of possible involved entities. Then, this basis was specified and verified in external expert/manager interviews. This was done by asking which entities are involved in enterprise mobility, challenging whether certain earlier mentioned entities are valid and asking how entities should be named. The grouping and naming of identities remains arguable as this can be done in multiple ways, using different names. However, after having multiple tiers of verification, it can be concluded that all possible involved entities are identified and part of the explained groups. The four defined groups as shown in Figure 28: Entity groups, are further explained and scoped to define which entities are part of the group and which entities aren't.

Figure 28: Entity groups

(The blue entities represent internal entities and the green represent external entities.)

Enterprise Organization

The 'Enterprise Organization' contains all entities that have a role in providing or managing enterprise mobility in the broadest sense. Together with the IT department of the organization, the management of the organization that provides mobility and is responsible for the enterprise wide policy on mobility is the most important entity in this group. Based on ISO/IEC 27000 (2009) guidelines possible involved entities are listed and explained to scope the group and provide practical references to identify entities in this group:

- Board of directors: enterprise vision on mobility
- IT management: IT vision on mobility
- IT department: enrollment & support
- HRM: employee agreements & financial
- Legal: employee privacy & law compliance

The IT department is not classified as a different group but part of the 'enterprise organization' entity, as it is perfectly fits in the description of this group: 'providing and managing enterprise mobility'. Not part of this group are enterprise departments that do not influence enterprise mobility in any way, the employees that are using mobility and any organization that does influence enterprise mobility but is not part of the legal entity that is assessed. This group is involved because it enables and realizes enterprise mobility and thus influences the risks of enterprise mobility.

Employees

The employee group is very self-explanatory, but on the other hand very important in the scope of this research. Employees are the center of enterprise mobility as they are using the mobile devices and should be able to enforce the benefits of enterprise mobility by using it in their daily tasks. The group exists of all employees that are using one or more, company or personally owned mobile devices to execute work related tasks. Entities that do work for the organization but are not employees of the organization are not part of this group, but part of the 'Business partners' group. This group is involved because employees are the users of mobility and create threats and risks to the organization.

Business partners

The 'Business partners' group exists of all entities that work with or for the enterprise organization and make use of enterprise mobile solutions. Business partners are in the external environment of the organization as they are not part of the enterprise organization itself. The most common example is a supply chain or value chain partner that accesses the enterprise environment using a mobile device. For instance, when a partner delivers packages for an organization, he uses a smartphone to connect to the corporate environment and changes the status of the package. Besides, partners in the supply or value chain, temporary workers or consultants that make use of enterprise resources using a mobile device are also part of this group. Based on ISO/IEC 27000 (2009) guidelines possible involved mobile partners are listed and explained to scope this group:

- Supply chain partner: connected to enterprise via mobile interface
- Value chain partner: connected to enterprise via mobile interface
- Clients: only when connected to enterprise systems
- Temporary workers: using the corporate environment temporarily
- Consultants: using the corporate environment temporarily

Clients can also be part of this group when an extensive business relationship is established. When the organization connects clients to their corporate system using a mobile interface, the clients are considered as an entity that should be taken into account during the mobile risk assessment. However, consumer mobile apps are out of scope for this research as it is a completely different field of mobile usage and risk analysis. This group is involved as mobile connected business partners can be of risk to the organization when possible vulnerabilities in the mobile interface to enterprise resources are exploited.

Potential harmdoers

The most complex and extended group of entities is the Potential harmdoers group. This group represents all entities that are intentionally or unintentionally able to possibly harm any other entity that is involved with enterprise mobility by exploiting any (none) technical mobile vulnerability. Intentionally and unintentionally entities can have very different goals and are very different persons, nevertheless both entities are combined in the scope of a risk assessment as both parties are able to harm the enterprise organization. It is impossible to specifically identity all entities in this group, as one will never know which entities will try to perform harmful actions. Though, a list of known possible harmful entities is made to help identifying where possible threats can come from. This list is separated in two different areas, intentionally harmful entities (malicious entities) and unintentionally harmful entities. Intentionally harmful entities based on the theoretical findings in section 3.3 Mobile Security:

- Availability focused hackers: try to make the mobile device unusable for the user by for instance installing malware.
- Information focused hackers: try to steel (personal) information that is on the mobile device.
- Access focused hackers: try to impersonate a device and gain credentials to enterprise resources.
- Financially focused criminals: try to directly steel money from the user by for example using malware that charges money on the user's phone bill.
- Device focused criminals: try to steal and sell the physical device without being interested in the information that is on the device.

Unintentionally harmful entities:

- User: unintentionally spread sensitive information, ignore security policies or any kind of unaware harmful mobile actions
- User relatives (children): non-compliant entities that have access to the mobile device and spread sensitive information. Identified as one of the most underestimated risks by EMS01.

The list is not exhaustive and should be re-evaluated when assessing each entity group on possible threats. This group is involved as the underlying entities perform a direct threat to the organization or other involved entities.

The defined entity groups are part of the enterprise mobility domain and play different roles when assessing enterprise mobile risks. The four entity groups can create threats but can also be harmed by a threat. Further sections will elaborate on how these entities are involved and assessed in the M-RAM method.

5.3 Risk Assessment Process

This section provides an answer to the first two defined sub research questions: *SRQ1: Can traditional risk management processes, standards and models be used for enterprise mobility?* And *SRQ2: Which process steps should be taken to assess mobile risks and how should these steps be executed?* The answer to the first SRQ is mainly based on the evaluation of the theory in section 3.4 IT Risk Management and the 'Risk assessment' statements from experts. The answer on the second SRQ uses the output of the first SRQ, the 'Risk assessment' statements from external as well as internal experts and output from the SLR.

Evaluating traditional processes

IT risk assessment processes are used to assess different information assets. The discussed risk management and risk assessment artifacts in section 3.4 IT Risk Management are designed and used in different levels of risk management. Some artifacts are designed for very practical risk analyses were others contribute on high level risk management processes. The theoretical standards are discussed on their applicability for a mobile risk assessment process in order to form a basis for the M-RAM process.

COSO – The three dimensional COSO cube provides a high level view on risk management, the three explained steps 'Event Identification', 'Risk Assessment' and 'Risk Response' provide the steps that are related and part of the risk assessment. Despite that the COSO cube is very generally designed for the management of all kinds of information assets, the described process activities can be very useful for a mobile risk assessment process. The steps in Figure 29: Derived COSO process steps are derived from the integrated COSO framework. The blue steps are within the scope of the M-RAM process and define the basic steps of a risk assessment. The green step is part of the risk response step and is triggered by the output of the risk assessment and thus out of scope for the M-RAM process.

Figure 29: Derived COSO process steps

ISACA – The risk IT process model by ISACA remains on a very high level. The 'Risk Evaluation' is one of the three triangle components and contains a risk analysis activity. The model does not provide any risk assessment process but does explain that a risk analysis is part of the risk assessment and should always encounter the frequency and impact of a risk (ISACA, 2009). Furthermore, ISACA (2009) states that the risk assessment also contains preliminary and ancillary steps in order to identify possible risk scenarios (threats) and identify risk responses (controls). The process model also states that the current risk as well as the residual risk should be calculated. From these statements risk assessment process steps can be derived as shown in Figure 30: Derived ISACA process steps. Again, this process model is very general and not related to mobile risk assessments.

Figure 30: Derived ISACA process steps

SPRINT – The SPRINT method is a very practical and concrete risk assessment model which already includes process steps. The steps do not consider the actual calculation of risks and the acceptance of risks. The method is mostly used to assess information systems and has no relation to mobility. Figure 31: Derived SPRINT process steps' shows the derived process steps from the SPRINT method.

Figure 31: Derived SPRINT process steps

ISO – The theoretical chapter evaluates two different related ISO standards, the ISO31000 and the ISO27005 standard. The ISO27005 standard is not further discussed as the standard remains very high level and only explains three core steps for IT risk management. In contrast to the ISO27005 standard, the ISO31000 standard provides a detailed process for conducting an IT risk assessment. The process steps are elaborately described in the theory chapter and a derived version of the process steps are shown in Figure 32: Derived ISO31000 process steps. Like the other discussed risk assessment process steps, the ISO31000 risk assessment process is designed for general information asset usage and does not take any mobile considerations into account.

Figure 32: Derived ISO31000 process steps

IRAM – The IRAM model contains of very practical techniques to perform parts of a risk assessment. The model opposes a method to calculate the impact of a risk, the likelihood of threats and vulnerabilities and a method to determine which controls should be selected in order to mitigate the risk. The IRAM model will not be further used to determine the M-RAM process steps as the IRAM method is explained on a lower abstraction level and can not be compared to the other methods.

NIST – The NIST 800-30 publication defines concrete process steps to perform an IT risk assessment. The process steps are again developed for general IT asset assessments. However, NIST also published a special publication (800-124) on security guidelines for managing mobile devices in enterprise environments (Souppaya & Scarfone, 2013). This publication provides detailed areas for vulnerabilities and threats, but does not provide a risk assessment process for enterprise mobility. Instead, the publication refers to the risk assessment process of the 800-30 publication. For that reason, the process steps of the 800-30 publication are derived and shown in Figure 33: Derived NIST process steps.

Figure 33: Derived NIST process steps

OCTAVE – The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) provides three phases that include eight different steps. The seventh step incorporates the risk analysis, which aims to provide a defined risk profile for each asset. The OCTAVE model is developed to analyse threats and vulnerabilities on general information assets, mobility is thus not considered with this method. The derived steps in Figure 34: Derived OCTAVE process steps are bases on the process steps, mainly considering the risk analyses step.

Figure 34: Derived OCTAVE process steps

Reference process

The evaluated traditional risk assessment process models propose very comparable steps. Therefore a comparative matrix is used to compare the different steps of each method and create a reference method (Levantakis, Helms & Spruit, 2008). Table 5: Comparative matrix: Risk Assessment Methods provides a comparison of the different methods. The reference, also called super method, combines all methods into one super method that entails the most important steps of each method.

Activity	COSO	ISACA	SPRINT	ISO31000	NIST	OCTAVE	Reference Method
Asset classification			X	X	X	X	**X**
Threat & event identification	X	X	X	X	X	X	**X**
Vulnerability identification			X		X	X	**X**
Risk identification		X	X	X			
Risk quantification	X	X		X	X		**X**
Control analysis	X	X	X				**X**
Residual risk analysis	X	X					**X**
Define action plan	X	X	X		X	X	**X**

Table 5: Comparative matrix: Risk Assessment Methods

The ‘Risk identification’ step is not used in the reference method as it is not specific enough and will be incorporated with the ‘Risk calculation’ step. Furthermore, the reference method is visualized in Figure 35: Reference method: traditional risk assessment processes. The determined reference method is used as a basis for the M-RAM process, excluding considerations for mobile usage. The dark blue activities are all included in the reference method, where the light blue steps are not included as they were not specific enough.

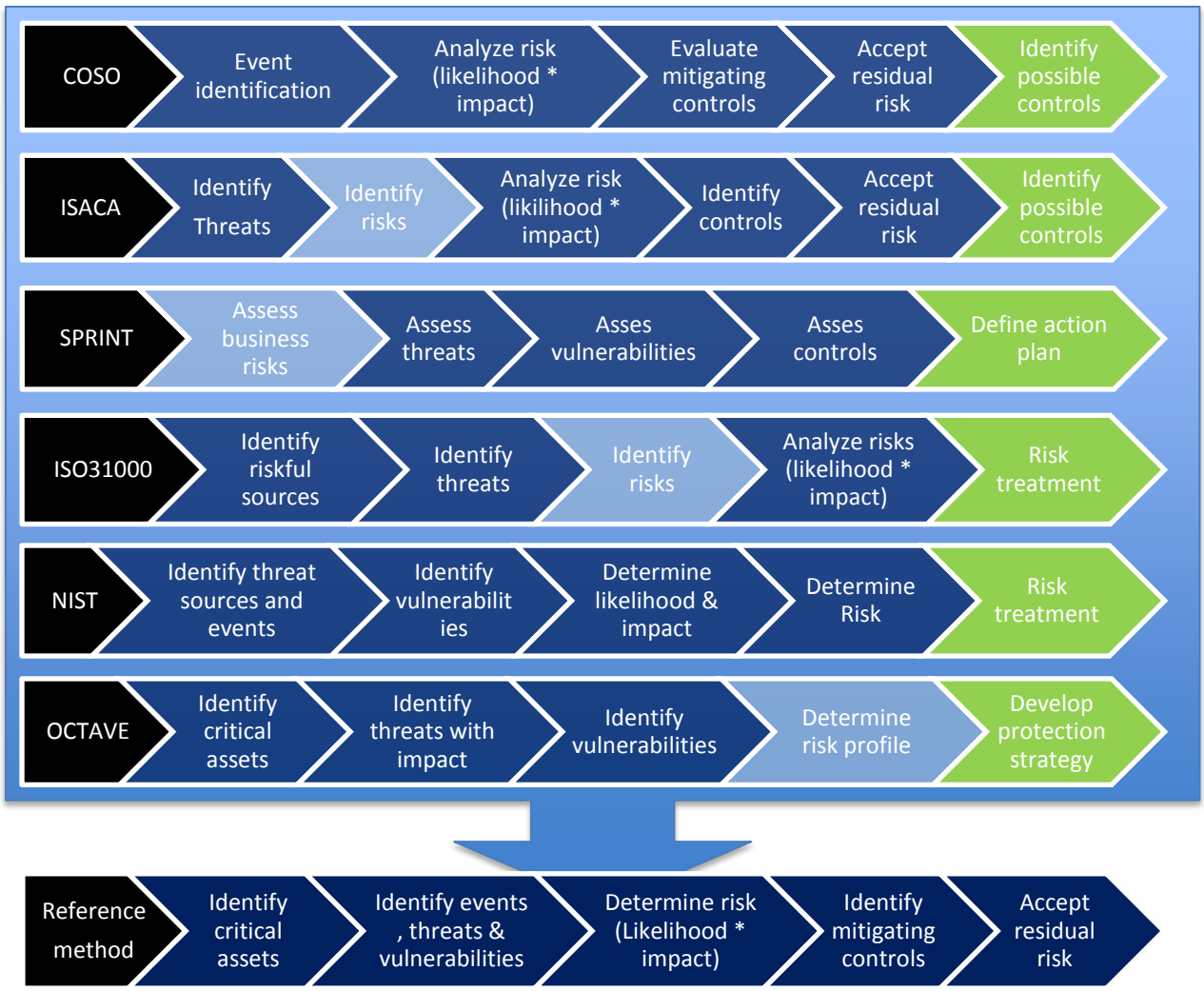


Figure 35: Reference method: traditional risk assessment processes

The Mobile Risk Assessment

The mobile risk assessment process is mostly based on the defined reference method, as mobile assets are very comparable to other information technology assets. However, small differences, complements and additions need to be considered when assessing the risks of enterprise mobility. Mobile security experts were asked to what extend they find the reference method suitable for a mobile risk assessment and where additions or changes are needed. Furthermore, statements from internal Deloitte experts, scientific as well as grey literature are considered to optimize the mobile risk assessment process. Each step of the defined reference method is considered and adapted to use in the context of mobility. A figure is used to provide an overview on how each step is adapted. Figure 36: Example step adoption provides an example on how these figures are used for each step.

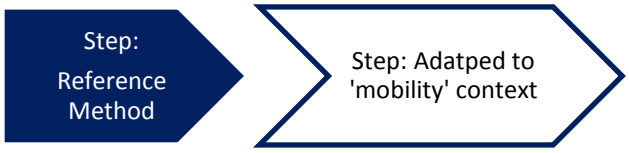
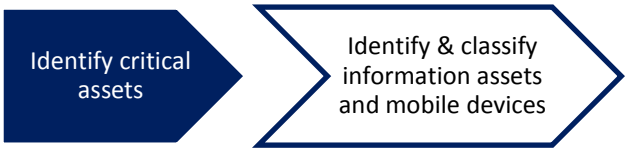
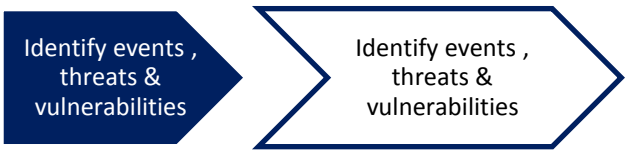


Figure 36: Example step adoption

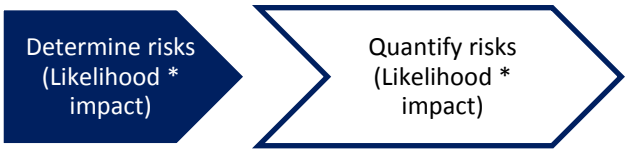
Mobiquity (2013) states that a mobile risk assessment should start with identifying the types of data, business processes and activities that are used, stored or accessed via mobile devices. MSM03 explained that information assets that are accessed or used by mobile devices and information that might be stored on mobile devices should be classified on integrity and confidentiality, in order to determine which information is allowed to be stored or accessed on certain mobile devices. Furthermore, MSM03 also stated that mobile devices should also be classified on their security measures and trustworthy. After doing these two classifications, the organization should decide which information classification is allowed on which device classification (MSM03). MSE08 added that one difference with a mobile assessment is that one needs to also classify the mobile device, where traditional assessment only focuses on the information assets. MSE12 states that the information that is stored on mobile devices and accessed by mobile devices should be classified using a business impact analysis in order to determine the risks of having certain information on mobile devices. Combining these statements leads in changing the 'Identify critical assets' step of the reference method to a more elaborate and further defined step named 'Identify & classify information assets and mobile devices'.



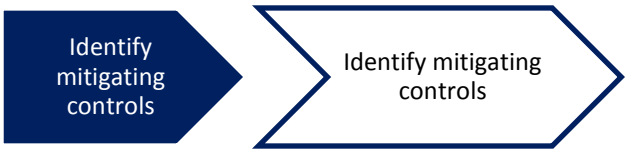
The second step of the reference method 'Identify events, threats & vulnerabilities' is often split into two separate steps 'threats & events' and 'vulnerabilities'. As events can lead to possible threats, vulnerabilities can trigger malicious parties to execute an event and vulnerabilities are responsible for possible threats the step should remain the same and not be split. The importance of this step in scope of a mobile risk assessment is validated by the interviewed mobile security managers and experts. MSM01 stated that threat and vulnerability analysis are done when assets change, the analysis are outsourced to external specialists as they have the most up-to-date knowledge. MSM02 uses the IRAM industry standard to identify threats and vulnerabilities on a regular basis and when assets are changed. Furthermore, the attack vectors described in section 3.3 Mobile Security verify the seriousness and need for identifying threats to the organization and vulnerabilities that can expose these threats.



Determining the risks that originate from the identified threats is a logical but never discussed next step. In order to quantify the inherent risks and residual risks a measurement method is needed (ISACA, 2009). The interviewed mobile security managers that do not outsource the risk analysis, all use a likelihood * impact analysis or an industry standard containing a likelihood * impact analysis. Mobiquity (2013) states that 'threat intelligence' should be done by different sources that estimate the likelihood and impact of each threat. MSE01 stated that mobile risk assessment should also be evaluated on their impact and likelihood. Furthermore, the special 800-124 publication on mobile security from NIST states that identified threats should be quantified on the likelihood and impact of a successful attack (Souppaya & Scarfone, 2013). The identified risk analysis step 'Determine risk (Likelihood * impact)' from the reference model will therefor remain almost unchanged for the mobile risk assessment process. The only change is the definition of the step, 'determine' is changed into 'Quantify' in order to specify that the risks will be evaluated using a quantitative method.



In order to determine what the residual risk is compared to the identified inherit risk, mitigating controls need to be identified. The reference method already contains the step 'Identify mitigating controls'. The approach to this step will be very different with a mobile assessment compared to



traditional risk assessments, as the attention areas for controls are very different. The difference in approach will be further discussed in section 6.2 . Despite the fact that the approach will be very different, this step also needs to be included with the mobile risk assessment process. Souppaya & Scarfone (2013) state that the security controls of mobility need to be identified in order to determine the residual risk and be able to evaluate whether further controls are needed. MSE12 stated that mitigating controls should be identified and related to the threats that are identified. The mobile risk assessment will also contain the 'Identify mitigating controls' step. Where and how mitigating controls can be identified will be explained in section 5.4 Attention Areas.

The last step of the reference model explains the acceptance of residual risk. By linking the identified mitigating controls to the quantified risks, residual risks can be quantified in order to know to what extend the taken controls mitigate the risks and be able to accept or not accept the residual risks. The difference with traditional risk assessment is that with mobile not only the residual risk is important for organizations, but also the impact on mobile usability and mobile innovation. As more

than 90% of the MSM's and 100% of the MSE's see a tension field between mobile innovation and mobile security, the impact on innovation and usability cannot be ignored. Therefor this step should incorporate a qualitative analysis that determines to what extend mobile innovations and mobile usability is tempered by the equipped mitigating controls. The 'Accept residual risk' step of the reference method is updated to 'Evaluate residual risks and innovation'.

The discussed and updated steps as shown in Figure 38: Core mobile risk assessment process defines the core process of the mobile risks assessment.

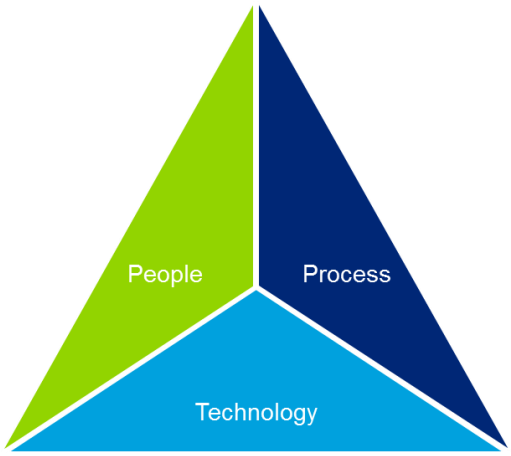
Figure 38: Core mobile risk assessment process

However, in order to conduct the mobile risk assessment a preliminary step is required. MSE01, MSE03 and MSE08 stated that a preliminary step is needed to define how a company is thinking about mobility and what their policy is regarding enterprise mobility. This knowledge is needed in order to put later analysis in perspective of the organization and its policy on enterprise mobility. Furthermore, it is important to ask the organization how mobility is used and research how mobility is really used by employees. This activity is very important as the demand and usage of employees often differs from the organizations policy. Not executing this activity would lead to a non-rigorous assessment. Therefore, the preliminary phase 'Identify policy, demand & usage' is added to the mobile risk assessment process. Moreover, a follow up step is defined to determine the scope of the assessment and provide means to follow up the output of the assessment. The follow up step contains the creation of an action plan. The action plan should be based on the residual risks that cannot be accepted and the consequences for mobile innovation and usability that cannot be accepted. This step is not part of the mobile risk assessment process, which is visualized in Figure 37: Preliminary & follow up phase. The approach to both the preliminary phase as the follow up phase will be discussed in section 6.2 Method.

Figure 37: Preliminary & follow up phase

5.4 Attention Areas

This section provides an answer to the first part of *SRQ4: How can mobile vulnerabilities and mitigating controls be categorized and identified?* The categorization of mobile attention areas is needed in order to guide the risk assessment steps in the right areas of mobility. Each determined attention area can contain mobile vulnerabilities as well as abilities to incorporate mitigating controls. A solid and rigorous categorization of mobile attention areas is a big challenge as different terminology as well as different aggregation levels can be used. Furthermore, each defined attention area has to be scoped and described in detail to ensure what vulnerabilities and mitigating controls are or aren't part of an attention area.



Multiple steps are taken to determine the final mobile attention areas. First, the aggregation level is defined. The well-known people, process and technology categorization (Chen & Popovich, 2003) is considered valid, but too high-level and not specific enough for the M-RAM artifact. Adding all possible attention areas from literature and expert interviews would lead to more than 20 different attention areas, which would make the desired M-RAM artifact obscure and unclear. To assure that the artifact remains clear and that attention areas are distinctive for mobility, a scope for the amount of attention areas is set. The final attention areas are based on (scientific) literature and expert interviews. The used literature and expert statements are now evaluated and considered in order to shape the final attention areas.

The 800-124 special publication of NIST defines seven different attention areas for mobile vulnerabilities and security controls. The seven different areas are listed and explained:

1. **Physical device security** – Mobile devices can be found in different public places and an organization should assume that a device is accessible by malicious parties. Therefore, physical authentication and data protection (encryption) should be in place.
2. **Untrusted devices** – Personally owned, unmanaged and rooted devices bring a great threat to the organization, controls for these threats can be BYOD restriction, technical enforced policies or company sandboxing.
3. **Untrusted networks** – External Wi-Fi and cellular networks that cannot be controlled. Data encryption and policies for not using unsecured networks are named as mitigating controls.
4. **Untrusted applications** – Third party apps that pose obvious security risks by using and accessing data in an unwished manner. White-black listing and sandboxing of applications are listed as mitigating controls
5. **Interaction with other systems** – Unsafe transaction of data with other systems. Mitigating controls as blocking services, encrypting connections and defining policies on which systems may be linked to which devices.
6. **Untrusted content** – Data from social networks, apps, QR-codes and other sources may include malicious code and can harm organizations. Location services are often used to trick users with malicious code, disabling location services is listed as a mitigating control.
7. **Location services & privacy** - The use of location services can complicate organizational security and personal's privacy. Disabling location services is the most obvious control.

The seven different attention areas are mostly focused on the technical side of mobile security and do not consider people or process areas. The Dutch National Cyber Security Centrum (NCSC) which is part of Ministry of Security and Justice has published safety guidelines for the usage of mobile devices in enterprise environments. The publication contains two documents that specify six different areas for mobile security guidelines (National Cyber Security Centrum, 2012). The first

document specifies high level guidelines, were the second document complements on these guidelines by providing detailed mitigating controls. The six different attention areas are listed and explained:

1. **User** – The guidelines define how 'the user' should work with mobile devices and what the pitfalls are in mobile usage. Losing the device, eavesdropping and careless usage of online storage are examples on how to use mobile devices.
2. **Policy** – General as well as device specific policies need to be defined. The general policy guidelines contain inter alia policies on data privacy, user awareness & training, device rooting and back-up intervals. The specific policies are not further explained but state that device specific policies should be determined.
3. **Device access** – Controls to prevent malicious parties from gaining data when having physical access to a device. Data encryptions, passcodes, remote locking/wiping are examples of controls in this attention area.
4. **Application** – This attention area focusses on the security of mobile apps. Controls focus on software updates, privacy, rights to access resources and other app related controls.
5. **Mobile platform** – This attention area is not detailed in the publication but states that the designs on MDM and MAM (Mobile Application Management) systems should be seen as a separate attention area where vulnerabilities on system level can be identified and controls can be arranged.
6. **Network & data** – This attention area focusses on how data is send over networks and how different network connections should be secured. Typical controls are no automatic or untrusted Wi-Fi networks, VPN connections, managed Bluetooth & NFC and limited use of network connections.

The detailed controls of the NCSC publication are not further discussed in this section the aim is to determine mobile security attention areas. Citrix (2013) distinguishes four attention areas for mobile, focusing on the technical side of mobile security. Each of the four areas (1) **Devices**, (2) **Apps**, (3) **Network** and (4) **Data** needs to be monitored, controlled and protected. Citrix (2013) provides controls that can help monitor, control and protect each of the four attention areas. On behalf of the Information Security Forum (ISF), Davis, Nowak & Vrhovec (2011) define four major attention areas for mobile 'consumer' devices as shown in Figure 39: Four attention areas of Mobile Security (ISF, 2011). The publication defines challenges (vulnerabilities) as well as solutions (mitigating controls) for each attention area. The challenges and solutions are divided over **(1) Governance, (2) Devices, (3) Applications & data** and **(4) Users.**

Figure 39: Four attention areas of Mobile Security (ISF, 2011)

The different attention areas, as published by the different institutes as well as the considerations made by experts are summarized in Table 6: Attention Areas. Most attention areas are backed by the theoretical sources as well as the expert statements. **Device, App, Data** and **User** are the four areas that can directly be accepted as all theoretical sources and all experts back them.

Attention Area	Theory	Expert
Devices	NIST 800-124, ISF, NCSC	MSE01, MSE02, MSE03, MSE07, MSM05
Apps	NIST 800-124, ISF, NCSC	MSE01, MSE02, MSE03, MSE07, MSM05
Data	NIST 800-124, ISF, NCSC	MSE01, MSE02, MSE03, MSE07, MSM05
Governance, processes, policy	NIST 800-124, ISF	MSE01, MSE02, MSE03, MSE07, MSM05
Users	NIST 800-124, ISF, NCSC	MSE01, MSE02, MSE03, MSE07, MSM05
MDM Platform	NCSC	MSE03, MSE07, MSM05
Network	NIST 800-124, NCSC	
Privacy, compliance, regulation	NIST 800-124	MSM02, MSM05

Table 6: Attention Areas considerations

Governance and policy are terms that are a bit vague and require for more explanation. Furthermore, the considered governance and policy controls can always be considered part of the other attention areas, mostly processes, users and privacy. In order to keep the M-RAM artifact clear and rigorous, 'policy' and 'governance' are not included as separate attention areas. 'Processes' is also a somehow general term but nevertheless a very important area in order to control the use of mobile devices. For this reason 'Processes' is specified as 'Control processes', which was also advised by MSE07. 'MDM Platform' is not backed by every theoretical publication, which can be explained by different expert statements. MSE03, MSE07 and MSE08 stated that the MDM platform, a MDM system can have different vulnerabilities that are often not considered. These statements and the NCSC publication substantiate the addition of the 'MDM Platform' attention area. The 'network' attention area is a discussion point as it is mostly seen as part of the 'Data' area. As the vulnerabilities and controls are highly related to each other, network is merged with data to form one attention area 'Data & Network'. Privacy, compliance and regulation are areas that are also often not considered. Especially BYOD constructions and geographical boundary crossing provides great risks and challenges for mobility. Privacy issues can be a threat for the user but also become a threat for organizations when one is not compliant with privacy regulations. Therefore, 'Privacy & regulations' is added as a seventh and last attention area. An overview of the final attention areas can be found in Figure 40: Final Attention Areas. The colors refer to the earlier explained higher-level people (Green), process (Dark blue) and technology (Light blue) model (Chen & Popovich, 2003). Except the relation to the people, process and technology model, there is no direct relation between the different attention areas.

The names for the final attention areas are chosen to be self-explanatory for the majority that will use the M-RAM artifact. However, a brief explanation of each area is needed to determine the scope of each area and be able to assess which vulnerabilities and controls are or aren't part of an attention area. Each attention area and its context are elaborated, vulnerabilities and controls are later explained in section 6.2 Method.

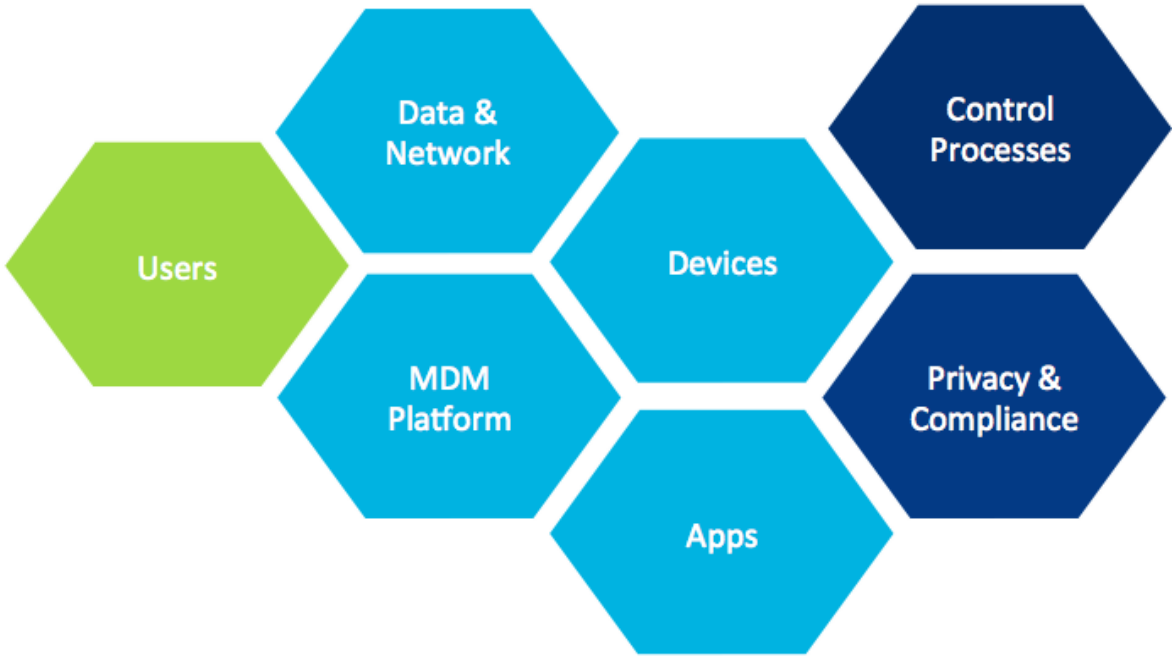


Figure 40: Final Attention Areas

Users

This attention area contains all threats that are initiated by the people that make use of the mobile devices that are linked to the evaluated organization. Furthermore, all mitigating controls that are appointed to positively influence the user on their mobile usage are part of this attention area.

Privacy & Compliance

This area exists of threats to the evaluated organization as well as the employees. Threats that somehow can violate the privacy of employees are part of this area as well as threats that can lead to consequences to the organizations for not being compliant with any (inter)national legislation on privacy, encryption or other mobile device related laws. All controls that prevent the violation of personal's privacy or violation of legislation by the evaluated organizations are also part of this attention area.

Devices

This attention area contains all vulnerabilities that can be identified on the physical hardware and operating system of the mobile devices that are used within the evaluated organizations. All mitigating controls that are based on the physical hardware or operating system of these devices are also part of this area.

MDM Platform

This attention area contains all vulnerabilities that can be found in systems that manage mobile devices (MDM) and systems that enable services that are used on mobile devices. Installed controls that mitigate vulnerabilities on platform level are also part of this attention area.

Apps

This attention area contains all vulnerabilities that can be found in any app (self-developed or third party) that is running on a mobile device that is used within the assessed organization. Controls that are installed to mitigate these vulnerabilities, black/white list apps or manage the rights of apps are also part of this attention area.

Data & Network

This attention area contains all threats that are directly related to the exposure or loss of enterprise data (via any mobile network connection). Controls that are installed in order to mitigate the possibility of exposing or losing enterprise data (via any network connection) are also part of this attention area.

Control Processes

This attention area contains all threats that are opposed by organizational processes that are not or not efficient arranged to manage the use of mobile devices. Introduced or optimized processes that are installed to mitigate these threats are also part of this attention area.

6 M-RAM: Mobile Risk Assessment Method

The M-RAM (Mobile Risk Assessment Method) is developed to assess organizations on the risks that originate from their enterprise mobile usage. M-RAM should make organizations aware of the risks that they are taking, what they are doing to mitigate these risks and if these mitigations are enough so that the taken residual risks can be accepted. The M-RAM exists out of three core components, entities, attention areas and the risk assessment process. This chapter explains how these components are related following step 10 of the research process and how the method should be used, following step 11 of the research process.

6.1 High-level Approach

Section 5 Artifact Components introduced the different components of the M-RAM artifact. This section explains how the three explained components are related to each other. The risk assessment process is the core of the M-RAM artifact and should be followed from left to right when executing the mobile risk assessment method. The involved entities and attention areas are both supporting the explained process steps. The involved entities are input to the mobile risk assessment process by providing information about policy, usage, demand, information assets and mobile assets. Furthermore, during the risk assessment process the involved entities are evaluated on their influence of possible threats to the enterprise organization. The explained attention areas provide guidance when identifying threats, vulnerabilities and mitigating controls during the risk assessment process. It is important that each area is considered during the process steps as indicated by the blue arrows in Figure 41: High-level M-RAM. Each attention area contains of guidelines that can be related to threats, vulnerabilities as well as mitigating controls. The actual guidelines are further explained in section 6.2 Method. The High-level approach as shown in Figure 41: High-level M-RAM provides an overview of the M-RAM artifact and is used to communicate the M-RAM approach.

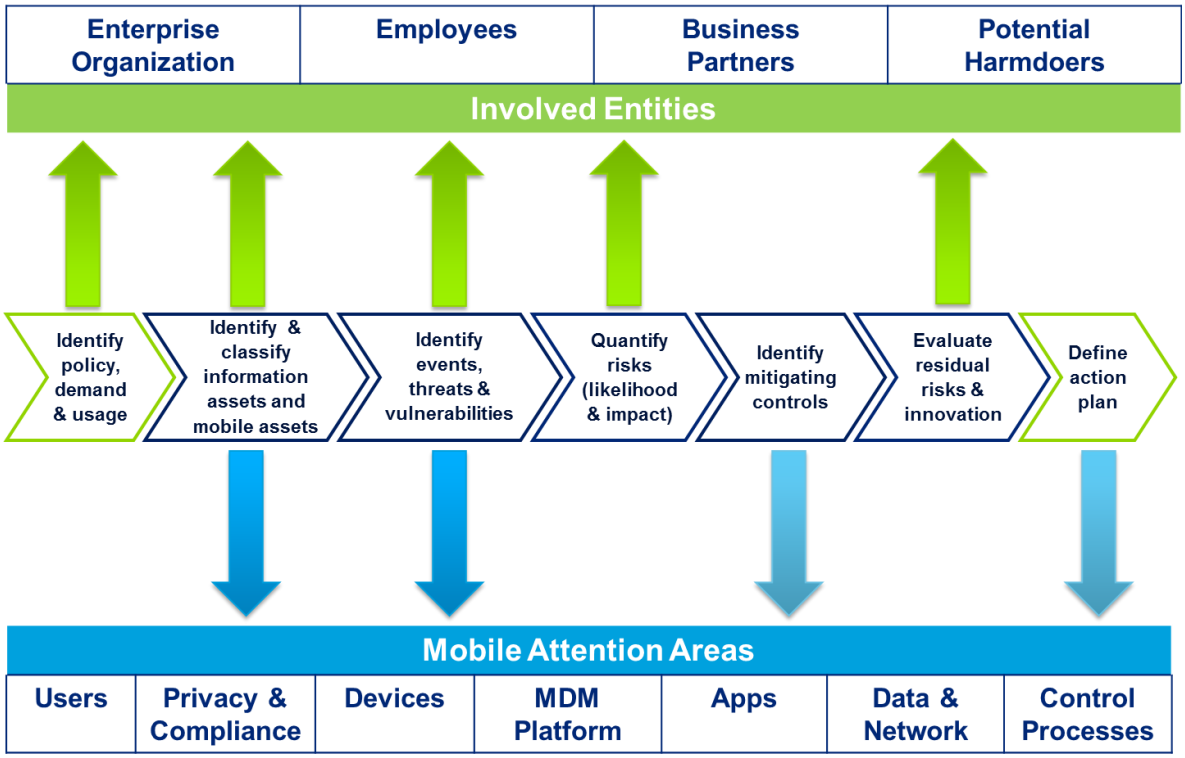


Figure 41: High-level M-RAM

6.2 Method

This section explains a practical interpretation for the Mobile Risk Assessment Method (M-RAM) and inter alia answers *SRQ4: How can mobile vulnerabilities and mitigating controls be categorized and identified?* This interpretation is very suitable to execute the M-RAM assessment; nevertheless other interpretations can be used to execute the M-RAM assessment. The method is explained by providing activities to execute each step of the risk assessment process. Furthermore, the method is complemented by explaining how the 'involved entities' are involved with each process step and by providing guidelines in each attention area for each process step that considers the identified attention areas.

The activities of each step are based on the techniques of the evaluated traditional risk assessment methods explained in section 3.4 IT Risk Management and the expert statements from experts. The provided attention area guidelines are not exhaustive and only valid for the current (2013) maturity of mobile security. The guidelines are based on security control publications of different research organizations, consulting organizations and expert statements. The guidelines aim to provide the risk assessor guidance in the identification of threats, vulnerabilities and controls.

Figure 42: M-RAM Work program provides an overview of the complete work program, a sharper image of the work program can be found in Appendix L – M-RAM work program. The figure shows which activities can be executed in parallel (identified by grey tones and indentations), which activities are dependent of earlier activities and which activities include a signing point (results that have to be signed by the case organization). Furthermore, the figure indicates which actors (internally as well as externally) need be involved in which activity. As this work program will be used in the case study described in section 7.1 Case , an indication of the needed hours for each activity is determined and provided in the work program. Each process step and underlying activity of the M-RAM artifact is explained elaborately in this section.

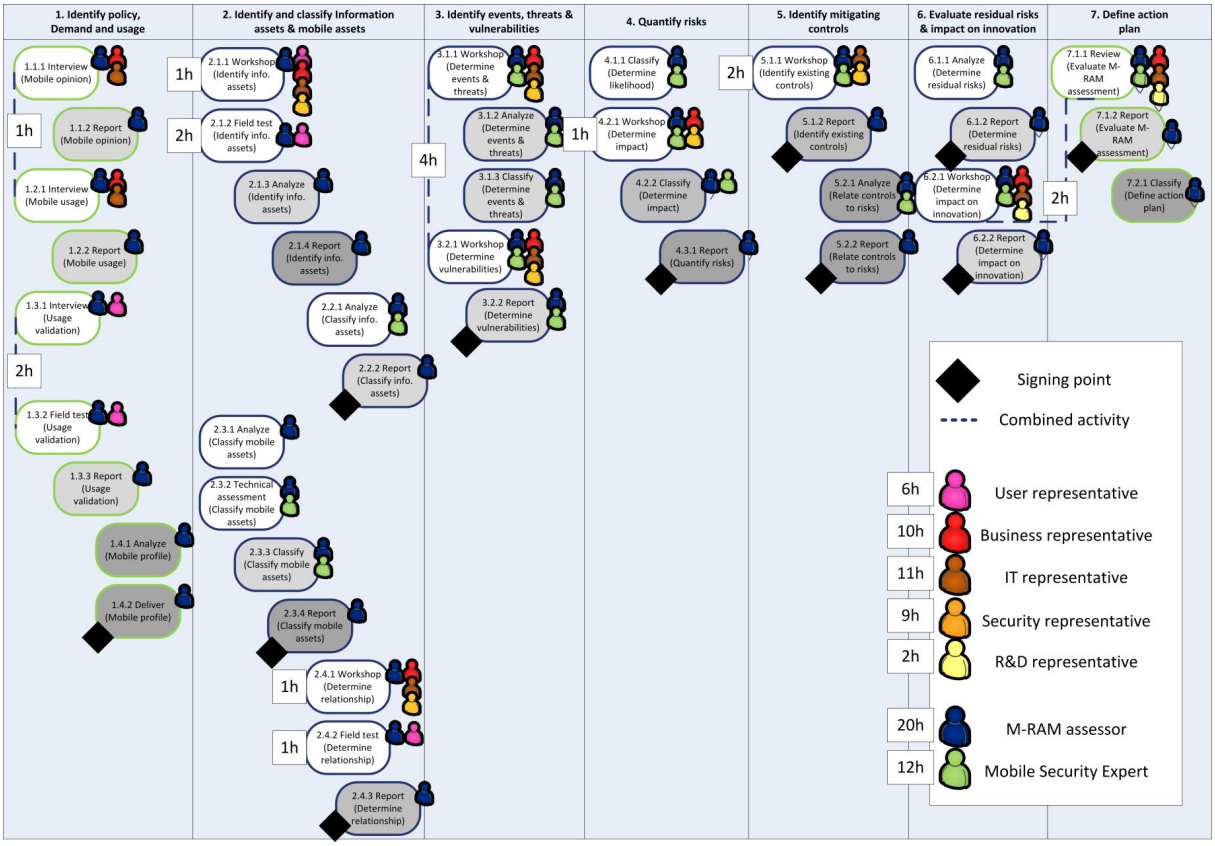


Figure 42: M-RAM Work program

1: Identify policy, demand and usage

This preliminary phase is used to create a 'mobile' profile of the assessed organization. Three main activities can be distinguished. First the opinion on mobility by the management of the company is identified. Secondly, the management of the organization is asked about how mobility is used. In order to validate the second activity, the last main activity examines the provided usage profile, by asking users on their demand and usage. Each activity and underlying sub activities are explained on a level that enables the M-RAM assessor to conduct the assessment.

1.1: Mobile opinion

1.1.1: Interview: Conduct two interviews, one with the 'business' and one with the IT department of the assessed organizations to assess the organizations opinion on enterprise mobility. The following questions could be used:

- *What does your organization want to achieve with the use of Enterprise Mobility?*
- *Is enterprise mobility a strategic asset or an infrastructure part for your organization?*
- *Are mobile devices used for supportive processes, primary processes or both?*

1.1.2: Report: Merge and compare the interview data and determine the mobile opinion of the assessed organization.

1.2: Mobile usage

1.2.1: Interview: Conduct two interviews, one with the 'business' and one with the IT department of the assessed organizations to assess the organizations mobile usage. The following questions could be used:

- *How are mobile devices (smartphones and tablets) supplied and who is paying for the device and carrier contract?*
- *Are users allowed to bring their own device for business purposes and connect to the organization's network?*
- *Can users use their own device for business purposes and connect to the organization's network?*
- *Can you provide a list of (approved) business activities (including: mail, agenda, contacts, web portals, document sharing, chat, people finder, supportive and primary applications) that are executed on mobile devices?*
- *Is application management enforced or are there guidelines for which applications may be used and which not?*
- *Who is responsible for mobile business and mobile usage?*
- *Who is responsible for mobile security?*

1.2.2: Report: Create a document that explains how the organization uses mobile devices from the organization's perspective.

1.3: Usage validation

1.3.1: Interview: Conduct a number of interviews (approximately 3) with mobile users. The following questions could be used:

- *How does the organization provide mobile devices and who is paying for the device and the carrier contract?*
- *What do you use your mobile device for (Applications, processes, tasks)?*
- *What would you like to use your mobile device for and why is this not possible?*

1.3.2: Field test: Inspect a sample (approximately 5) of the user devices checking:

- Device and OS version
- Device owner
- Installed applications
- Enforced policies

When a MDM system is in place a report can be exported to determine the actual usage of the organization.

1.3.3: Report: Determine how mobile devices are actually used by combining the interview results with the field test results.

1.4: Mobile profile

1.4.1: Analyze: Evaluate and compare the identified results of activity 1.2.2 with the output of activity 1.3.3. Analyze and research the differences.

1.4.2: Deliver: Create a 'Mobile profile' based on the template provided in Appendix B – Mobile profile. The mobile profile consists of the mobile opinion of the organization and the mobile usage of the organization.

2: Identify and classify information assets & mobile assets

'What are the crown jewels that need to be protected?'

The first step of the actual M-RAM is identifying and classifying information as well as device assets. The goal of a risk assessment is to determine how well your information assets are protected and how big the risk is that these assets will be compromised. Identifying the assets that need to be protected is the basis for conducting a risk assessment. Classifying information assets provides understanding on how important certain assets are and how well they need to be protected. The second classification is focused on the devices. Most organizations use multiple devices with different security measures and different trustworthy levels. Classifying these devices using trust levels provides insight on which information one would allow on a device. In order to correctly execute this step, the definition of the different assets needs to be explained;

Information asset: *Every business related information (source) or information system that can be accessed by a mobile device or can be stored on a mobile device.*
Mobile asset: *Every mobile device type (manufacturer, model and OS version) following the definition from '3.2 Mobility' that can somehow be linked to enterprise information.*

2.1: Identify information assets

2.1.1: Workshop: A workshop should be organized to determine the different information assets that can be accessed by mobile devices or can be stored on mobile devices. Participants of the workshop should represent the business, security, IT and the user group. The following information assets can be used as a discussion list to determine actual information assets:

- *Stored on device*
  - *Email (attachments), contacts and appointments*
  - *Document sharing apps*
  - *Customized apps*
  - *Voice, video and photo memo's*
- *Accessed by device*
  - *Document sharing*
  - *Intranet*
  - *ERP modules*
  - *Organization specific information systems*

2.1.2: Field test: Inspect a sample (approximately 5) of the user devices checking whether the in the workshop identified information assets are stored on devices and if the specified information assets can be accessed from devices. Also inspect (by asking the user) if other information assets are stored on the device and if the device is able to access other information assets.

2.1.3: Analyze: Evaluate the workshop and field test output and determine whether there are differences between both outputs. Also assess the results based on earlier experience and common mobile information assets in order to be complete.

2.1.4: Report: Report the final set of information assets using the template in Appendix C – Information assets.

2.2: Classify information assets

2.2.1: Analyze: Evaluate each identified information asset in step 2.1 on confidentiality and for instance use the information classification from Perkins (2013) to classify each information asset:

- ***Confidential*** *– strategic information*
- ***Restricted*** *– only accessible for a selected group or person*
- ***Internal Use*** *– may be used by all involved employees*
- ***Public*** *– not restricted and available for public use*

The classification needs to be accepted by the business owner of the information asset.

2.2.2: Report: Report the final set of information assets using the template in Appendix C – Information assets.

2.3: Classify mobile assets

2.3.1: Analyze: Use and analyze the report from step 1.3.3 to determine the different devices and OS versions that are distributed and used within the assessed organization.

2.3.2: Technical assessment: Assess each identified device + OS combination on standard security requirements. The following security requirements can be used as a basis for this assessment:

- *Authentication (No authentication, pin, advanced pin, fingerprint)*
- *Encryption (No encryption, partial encryption, app encryption, full disk encryption)*
- *Connection (No VPN, OS VPN, per app VPN)*
- *Remote control (No control, location identification, remote alert message, remote lock, complete device wipe, segmented wipe)*

2.3.3: Classify: Evaluate each identified mobile device in step 2.3.1 on device trustworthy, OS trustworthy and the results from 2.3.1. Then classify each device + OS combination in a predefined classification. The following categories can be used for this classification (MSM03, 2013):

- ***Trusted*** *– devices that are compliant with security requirements and trusted*
- ***Managed*** *– devices that can be managed, contain advanced security measures, but are not completely trusted*
- ***Basic*** *– devices that contain basic security measures*
- ***Not supported*** *– non trusted devices*

The classification needs to be accepted by the IT and security department.

2.3.4: Report: Report the final set of mobile assets using the template in Appendix D – Mobile assets.

2.4: Determine relationship

2.4.1: Workshop: Conduct a workshop with representatives from business, IT and security units to determine which information asset classifications are allowed on which mobile asset classifications. Table 7: Asset relationship example provides an example of the relations between information and mobile assets that can be explained.

	Confidential	Restricted	Internal Use	Public
Trusted	x	x	x	x
Managed		x	x	x
Basic			x	x
Not supported				x

Table 7: Asset relationship example

2.4.2: Field test: Inspect a sample (approximately 5) of the user devices checking whether the in the workshop identified asset relationships are valid. Create another table as explained in 2.4.1 to explain the determined relationships from the field test.

2.4.3: Report: Determine the differences between the workshop output and the field test output, then report the actual (field test) relationships and the differences with the workshop results (attention points).

3: Identify events, threats & vulnerabilities

The third step of the M-RAM artifact helps determining the threats that are opposed to the organization. These threats are initiated by events and mostly realized by exposing vulnerabilities. The different activities in this step require analysts with extensive knowledge on mobile security. Therefor the quality of the output of this step mostly depends on the involved analysts. Furthermore, the right business representatives need to be involved in order to make a rigorous impact estimation of the identified threats.

3.1: Determine events and threats

3.1.1: Workshop: A workshop should be organized to determine the possible external as well as internal events that can threat the organization. Participants of the workshop should represent the business, security and IT. The following external and internal events can be used as a discussion list to determine the actual possible events:

- *Internal (Organization and employees)*
  - *Employee loses device*
  - *Employee leaves organization*
- *External (Business Partners and (Potential harmdoers)*
  - *Partner or client misuses mobile access*
  - *Relative unintentional accesses or distributes confidential data*
  - *Malicious entity uses malware to gain access to information on the device or to access enterprise information sources from the device*
  - *Malicious entity uses the physical obtained device to access information on the device or to access enterprise information sources from the device*
  - *Malicious entity uses social engineering to access information on the device or to access enterprise information sources from the device*
  - *Malicious entity uses unsecure networks to access information on the device or to access enterprise information sources from the device*

3.1.2: Analyze: The identified events in step 3.1.1 need to be analyzed to determine which threats are triggered by the identified events. Appendix E – Guidelines for threats, vulnerabilities & controls provides a list of possible threats that need to be considered. The expertise of the assessor needs to complement this list as the list is not exhaustive because threats are constantly changing.

3.1.3: Classify: Each threat has to be evaluated whether they affect Confidentiality, Integrity and Availability of mobility and information used with mobility (ISF, 2013). Appendix F – Threat classification provides a threat classification template. The classification should be done by a security expert in order to make a realistic classification.

3.2: Determine vulnerabilities

3.2.1: Workshop: A workshop should be organized to determine the vulnerabilities in each attention area of the M-RAM artifact. Participants of the workshop should represent the Security, IT and experts on mobile security. Each of the seven attention areas (Users, Privacy & Compliance, Devices, MDM platform, Apps, Data & Network and Control Processes) need to be explicitly considered based on the following starting points:

- General known vulnerability guidelines (Appendix E – Guidelines for threats, vulnerabilities & controls)
- Organizations & system specific vulnerabilities (E.g. Devices, OS, MDM, policies)
- Threat playbook analyses (Identify vulnerabilities based on threats)

Depending on the knowledge of the workshop participants multiple iterations may be needed to determine all identifiable vulnerabilities in each attention area.

No	Threat	No	Vulnerability	Area
1	Hacking	1	No drive encryption	Device
		2	Get around passcode	Device
		3	Unsecured WiFi allowed	Data & Network
2	Denial of Service attack	4	MDM IP publically available	MDM Platform

3.2.2: Report: Relate identified vulnerabilities to identified threats by assessing if a vulnerability can be exposed to realize a threat. Report a list of threats using the template in Appendix G – Threat Vulnerability Analysis.

4: Quantify risks

By determining and combining the likelihood and impact of the identified threats, risks are quantified in this step. The likelihood of a threat can best be identified by security experts, where the impact of threats can best be identified by the business of the organization. This step proposes means to quantify the risks regarding enterprise mobility, but this can also be done using different classification methods.

4.1: Determine likelihood

4.1.1: Classify: Use the threat and vulnerability classification from Appendix H – Risk quantification to determine the likelihood of each threat. The likelihood will be determined on a scale from 1 (low) to 5 (high). The analysis should be conducted by a security professional that is able to determine the likelihood based on the identified threats and linked vulnerabilities.

4.2: Determine impact

4.2.1: Workshop: A workshop should be organized to determine the impact of threats to the business. The workshop should contain representatives from the business that are able to assess the impact of a threat on the organization, and security professionals that are able to explain the threat to the business. The workshop should determine the impact of threats based on financial loss to the organization.

4.2.2: Classify: The output is used to classify the impact of threats in different scales. The scales 1 (low) to 5 (high) can be related to financial loss of the assessed organization by determining a maximum amount of lost money to each scale. This classification is case (organization) specific and need to be determined in agreement with the organization. An example of such scale classification could be:

1. *€ 1,- to € 1.000,-*
2. *€ 1.000,- to € 10.000,-*
3. *€ 10.000,- to € 100.000,-*
4. *€ 100.000,- to € 1.000.000,-*
5. *€ 1.000.000,- to € 10.000.000,-*

4.3: Quantify risks

4.3.1: Report: Quantify each risk by multiplying the likelihood times the impact of each classified threat. Use the template from
Appendix H – Risk quantification to report the quantified risks.

5: Identify mitigating controls

The fifth step of the M-RAM artifact identifies the controls that are in place to mitigate the risks that originate from mobility. Each attention area of the M-RAM artifact is checked for possible installed

No	Threat	No	Vulnerability	Area
1	Hacking	1	No drive encryption	Device
		2	Get around passcode	Device
		3	Unsecured WiFi allowed	Data & Network
2	Denial of Service attack	4	MDM IP publically available	MDM Platform

controls as well as general known controls and controls based on threats. In order to define how the controls influences the identified risks, controls are linked to risks and analyzed on their mitigating force to risks.

5.1: Identify existing controls

5.1.1: Workshop: A workshop should be organized to determine the mitigating controls in each attention area of the M-RAM artifact. Participants of the workshop should represent Security, IT and experts on mobile security. Each of the seven attention areas (Users, Privacy & Compliance, Devices, MDM platform, Apps, Data & Network and Control Processes) need to be explicitly considered based on the following starting points:

- General known control guidelines (Appendix E – Guidelines for threats, vulnerabilities & controls)
- Organizations & system specific controls (E.g. Devices, OS, MDM, policies)
- Threat playbook analyses (Identify controls based on threats)

Depending on the knowledge of the workshop participants multiple iterations may be needed to determine all controls in each attention area.

5.1.2: Report: A list of controls, categorized in the M-RAM attention areas should be reported as a basis for step 5.2.

5.2: Relate controls to risks

5.2.1: Analyze: The output of the workshop in activity 5.1.1 should be analyzed in order to relate each control to one or multiple risks. A security expert, supported by the IT department and security department of the assessed organization, should do the analysis. Furthermore, the mitigating force on likelihood or impact of each control to each risk should be analyzed in order to be able to determine residual risks.

5.2.2: Report: The 'risk – control' relation and the mitigating force of each control to threat should be reported using the template in Appendix I – Risk – Control relation. This template specifies the mitigating force on likelihood or impact by estimating how strong the control is (none, small, medium, big).

6: Evaluate residual risks & impact on innovation

6.1: Determine residual risk

6.1.1: Analyze: The residual risk can be determined by assessing the identified risks and the controls that mitigate these risks. For this analysis the output of

		2	Get around passcode	Device
		3	Unsecured WiFi allowed	Data & Network
2	Denial of Service attack	4	MDM IP publically available	MDM Platform

Appendix H – Risk quantification and Appendix I – Risk – Control relation should be used to determine how the controls influence and mitigate risks. A security professional, together with a business representative should determine how the likelihood and impact is influenced by the controls that are installed.

6.1.2: Report: The template in Appendix J – Residual risk should be used to report the residual likelihood and impact for each risk. The residual risk can then be calculated by multiplying the residual likelihood and the residual impact.

6.2: Determine impact on innovation

6.2.1: Workshop: A workshop should be organized to determine how installed controls can influence mobile usage and mobile innovation. Participants of the workshop should represent the business, IT and R&D (innovation) representatives. Input of the workshop can be:

- *Innovation themes (Appendix K – Impact on Innovation)*
- *Installed controls (Appendix I – Risk – Control relation)*
- *Mobile innovation plans (Business, R&D)*

6.2.2: Report: Based on different innovation themes (Appendix K – Impact on Innovation) the impact on mobile innovation possibilities should be determined by the business and R&D (innovation) representatives. Appendix K – Impact on Innovation can be used to report and explain the impact of controls to mobile innovation. The output of this report can later be used to define an action plan for mobile security & innovation.

7: Define action plan

7.1: Evaluate M-RAM assessment

7.1.1: Workshop: A workshop should be organized to evaluate the M-RAM assessment and determine if and what further actions should be taken. Participants of the workshop should represent the business, IT, Security and R&D (innovation) representatives. Possible focus points of the workshop could be:

- *Risk level (acceptable)*
- *Lacking security controls*
- *Future innovations*

7.1.2: Report: Create a report that evaluates the outcome of the M-RAM assessment. The report should be written so that it can be used in further action plans.

7.2: Define action plan

7.2.1: Classify: This step is not part of the M-RAM assessment but could be initiated when the organization determines that the assessment needs to be followed up. The action plan can contain of new project initiatives that are focused on mitigating mobile risks and managing mobile security.

7 Validation

This chapter aims to validate the designed M-RAM artifact and underlying approach, following the last step (12) of the defined research process. The validation is done by conducting a single case study in a real-life environment. The first section of this chapter explains how the case study organization is selected, how the case study is conducted and provides the results of the case study. The second section evaluates the case study results and the last section provides an overview of the final M-RAM artifact, based on the case study evaluation.

7.1 Case Study

Case company selection

The envisioned validation step of the research process was already discussed during the most of the interviews with mobile security managers (MSM). The MSM's were asked if their organization was willing to cooperate in a case study that would test the M-RAM artifact and approach. Different organizations were willing to cooperate in the case study and in their view, a free mobile risk assessment. However, due to an estimated throughput time of one month and limited time of this research project, it was only possible to conduct one case study. The following four requirements were set to determine the most suitable and interesting case study organization:

1) The 'mobile' maturity level should be at the right level, meaning that the organization uses mobile devices extensively, but is not yet mature in mobile security and mobile risk management.
2) In order to validate the assessment for different situations, the organization should use multiple different mobile devices and use mobile devices in multiple use cases,.
3) The organization should be an interesting target for malicious parties, meaning that the organization deals with information assets that can be of interest to external parties.
4) In order to get the needed support for the case study, the organization should be concerned about the risks that originate from their mobility usage.

Especially the third requirement really defined the difference between the different case study organizations, as the selected organization deals with very privacy sensitive information that can be of create value to external parties. The selected organization cannot be named, as the case study results contain sensitive information about the organization. Though, the following properties of the organization are listed to provide some contextual clearance:

- Industry: Government
- Size: 10.000 – 20.000 employees
- Mobile devices: > 5.000

In the rest of this thesis, the selected organization will be referred to as the 'case company'.

Organization & planning

The organization and planning of the case study was very important as all stakeholders had a very busy schedule and the duration of the total study was limited to six weeks. The work program (Appendix L – M-RAM work program) was used as a guide to determine who would fill the needed roles in the case study as listed in Figure 43: M-RAM roles. The 'Mobile security expert' role was filled by an experienced risk manager that has experience in different IT risk assessments. Furthermore, the work program was used to plan the different activities (workshops, interviews, field tests and technical assessments). Figure 44: Case study planning provides a high-level overview of the case study planning.

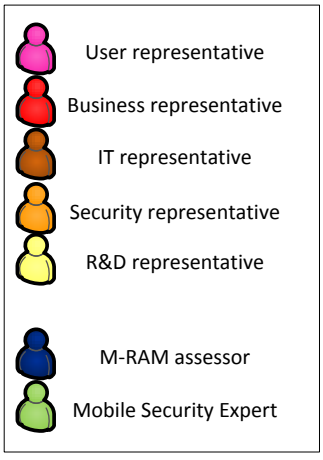


Figure 43: M-RAM roles

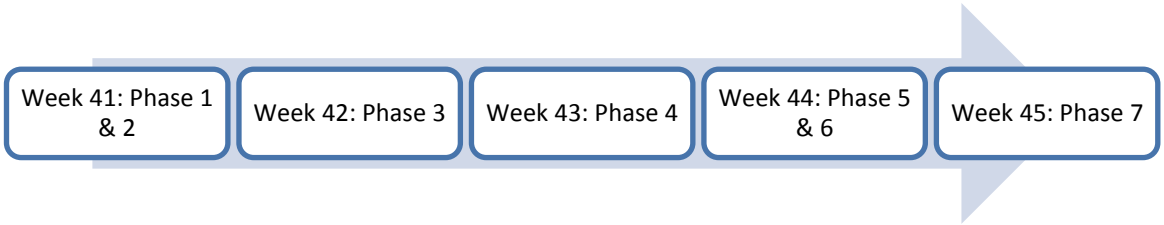


Figure 44: Case study planning

Results

The results of the case study following the interpreted method described in section 6.2 Method are processed and further explained in Appendix M – Case study results. The case study results are communicated to the assessed case company and accepted by the security officer of the assessed company.

7.2 Case Study Evaluation

In order to validate the proposed M-RAM artifact and the practical work program, the performed case study is evaluated. The structure and logic of the M-RAM artifact as well as the applicability of the M-RAM work program is discussed in this section.

The high-level approach worked out well as the steps defined in the risk assessment process are followed and evaluated as logical by the case study participants. However, the practical work program needed some adjustments in order to make the work program executable and logical.

Approach

The case study precisely followed the M-RAM approach and practical work program. The core of the M-RAM is the risk assessment process, which is evaluated first. The participants of the case study evaluated the process steps to be very logical and sound. However, the second step of the risk assessment process 'Identify & classify information & device assets' appeared to have the wrong order. As people think in devices and not in information assets, it was easier for the case study participants to start with identifying and classifying device assets and then proceed to the information assets.

The involved entities as well as the attention areas were very useful to the case study participants, for identifying the different threats, vulnerabilities and controls that were related to their mobility usage. There was no discussion on the four involved entities as these are pretty exhaustive. Considering the attention areas, it became very clear that one attention area was missing. Especially during the vulnerability analyses, different identified vulnerabilities could not be mapped to the seven attention areas. The vulnerabilities that could not me mapped were all about the non-controllable and varying environment of mobile devices, as shown in Table 12: Threats and linked vulnerabilities. As these vulnerabilities cannot be linked to one of the existing attention areas, a new attention area called 'environment' will be added to the high-level M-RAM approach.

Method

This section evaluates the practical M-RAM method by explaining the steps that were not optimal during the case study and therefore need to be adapted. An overview of the initial M-RAM method can be found in Appendix L – M-RAM work program.

Step 1: The first step of the M-RAM method remains unchanged, as there were no remarks to the conducted activities. However, it needs to be noted that the usage validation activities (1.3.1 & 1.3.2) are very important to validate the mobile usage and opinion of the organization and should never be skipped.

Step 2: As already explained in the previous section, the identification and classification of device assets should be done before the identification of information assets. Therefor the activities of step 2 should be followed in a different order. Furthermore, the technical assessment of activity 2.3.2 was not really suitable to determine all device assets, as it is really hard to technically assess all possible devices within the organization. The activity should be replaced with a workshop activity, so that all different devices are identified and classified. Still, the technical assessment activity 2.3.2 can be used to complement the workshop and verify the workshop results. A more practical change need to be made to the mobile device asset template as provided in Appendix D – Mobile assets. The template appeared to be too general and did not include critical information about the device's properties. Phase 2: Device Assets in Appendix M – Case study results provides a more elaborated template that is finally used in the case study and should be used in future usage of the M-RAM method. Finally, the most striking remark in the evaluation of step 2 is the unexpected outcome of the information asset identification and classification. The case organization had no specific restrictions for accessing or storing information on mobile devices, meaning that practically any corporate information asset could be accessed, when the mobile device was technically able to do so. This made the information asset identification and especially classification far less suitable, as theoretically the mobile devices could access any corporate information asset. As this outcome is very specific to the context of the case company, the method will not be adapted as it can still be very valuable in other cases.

Step 3: The most important remark in the evaluation of step 3 is the clarification of threats and vulnerabilities. It is really important that involved workshop participants have a good understanding on the difference between a threat and a vulnerability, before starting the workshops. Furthermore, there are no reasons to change any of the activities in step 3.

Step 4: At first the 4.1.1 activity should also be part of the workshop activity 4.2.1, as likelihood and impact is better classified when both are evaluated at the same time. Furthermore, it appeared that it is very important to select the right participants for the workshop in step 4. This is because there can be a lot of discussion on the values (1-5) of likelihood and impact. Concluding, it is important to exclude very strong characters in order to avoid endless discussions and make sure that the workshop chairman is able to manage the workshop participants.

Step 5 & 6: Step 5 and 6 are combined as it turned out that it is more practical and logical to combine parts of these steps in one workshop. At first, it is important to notice that the mitigating controls should be linked to the identified threats and that the controls should be described on a high level as further elaborated in Phase 5: Mitigating controls in Appendix M – Case study results. Secondly, we noticed that it is very logical to determine the residual likelihood, impact and risk directly after determining the controls that mitigate a risk. This means that the workshops of activity 5.1.1 should be combined with the activity of 6.1.1.

Step 7: The last step of the M-RAM method can be very different as it depends on how the assessed organization wants to follow up the outcome of the assessment. There were no changes made to the activities in step 7.

A general comment to the M-RAM method is that the quality of the outcome really depends on how much time is taken to execute activities and validate results and which stakeholders are involved with the execution of the M-RAM method.

7.3 Final M-RAM

Based on the case study evaluation, the M-RAM approach is extended with the new attention area 'environment'. The adapted M-RAM approach can be found in Figure 45: Final M-RAM Approach.

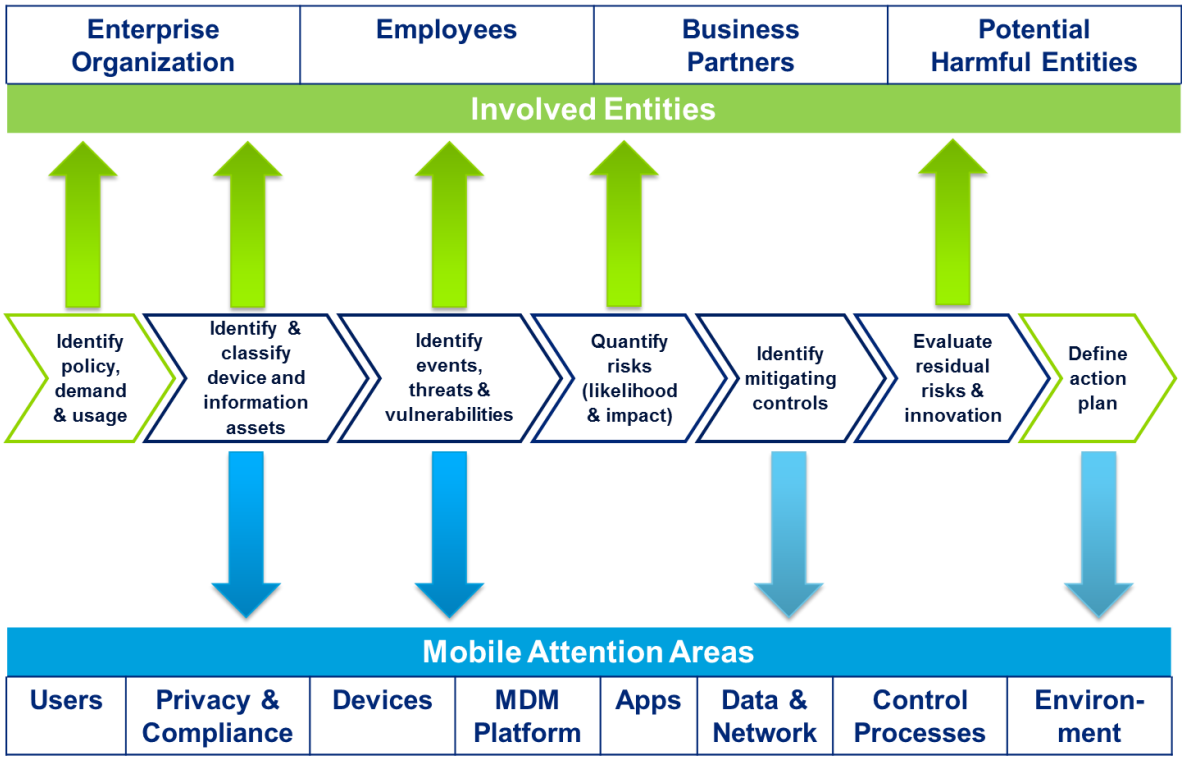


Figure 45: Final M-RAM Approach

Moreover, the M-RAM method or practical work program is adapted after the case study validation and an overview of the adapted work program can be found in Figure 46: Final M-RAM method overview, a sharper version can be found in Appendix N – Final M-RAM method (work program).

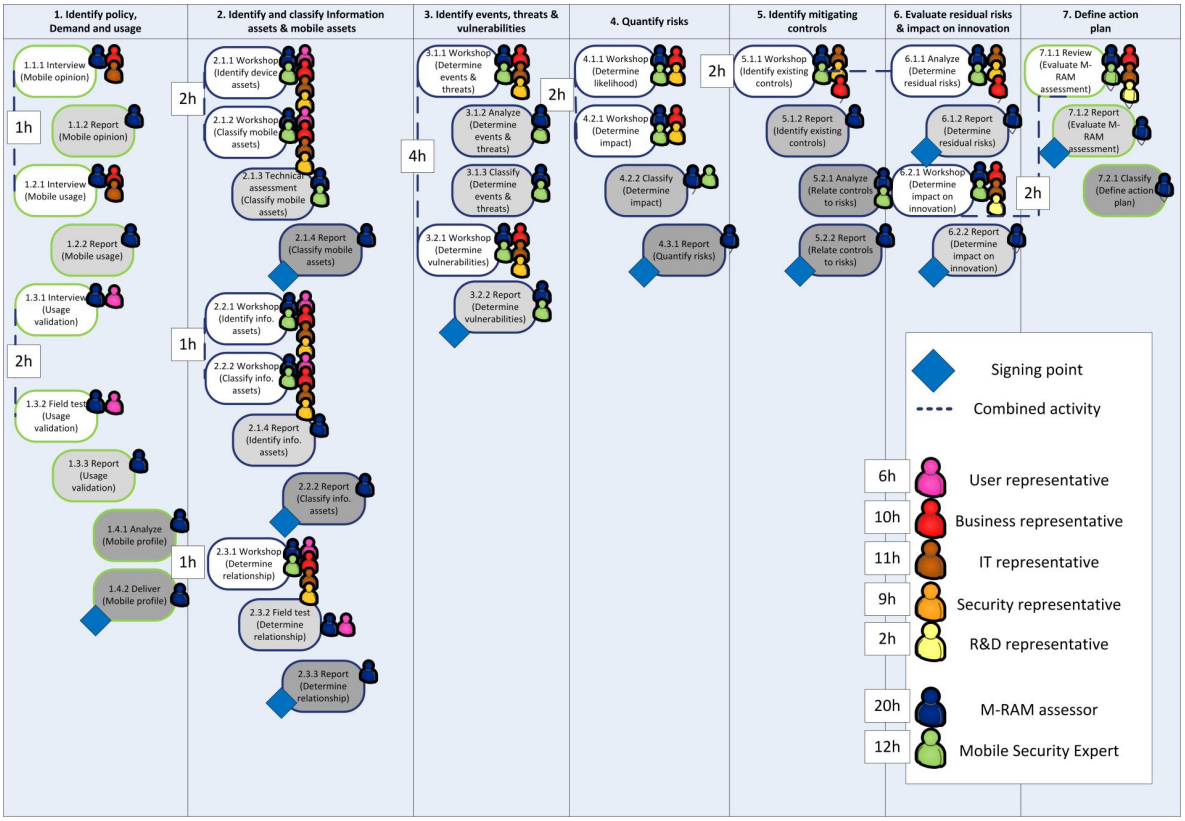


Figure 46: Final M-RAM method overview

8 Discussion and Conclusions

This chapter evaluates the research by stating the limitations of this research, concluding the research questions as stated in section 1.3 Research Question and explaining how this research can be continued in the future. Furthermore, different trends in the field of enterprise mobility are evaluated in order to understand the impact of such trends.

8.1 Limitations

The limitations of this research are described in order to provide the reader a good understanding of the value and soundness of this research. In general, it could be stated that the solely qualitative approach of data gathering by expert interviews is a limitation. However, a quantitative approach would not be feasible as the number of experts in this field is limited. Nevertheless, a number of 22 experts are interviewed, which provide an extensive set of qualitative data.

The first limitation is a demographic limitation; different sources state that the maturity of enterprise mobility in the Netherlands is very different compared to the maturity in other continents or countries like the United States (Cisco, 2012). As almost all expert interviewees are active in the Netherlands, the results of this research are limited to the Netherlands and thus not representative for other countries.

The validation of the M-RAM method also contains some limitations. Due to the time intensity of the M-RAM assessment, this research only contains a single case study. This limitation also triggers the limitation of external validity, which is probably the most important limitation to this research. The M-RAM assessment is only validated in one environment, not considering different sizes of organizations, organizations in different markets, organizations with different threat entities and organizations with a different vision or perspective of mobile usage.

Finally, M-RAM work program is based on limited sources, as there is no comparable work available and the approach is a practical interpretation of the theoretical M-RAM artifact. This research is limited to one practical interpretation of the M-RAM artifact, based on theory on traditional risk assessment methods and advice of risk assessment experts.

8.2 Conclusions

This section first provides an answer to the defined sub-research questions. Secondly, the main research question is answered and the total research project is discussed and evaluated.

Research Questions

SRQ1: To what extent can traditional risk management processes, standards and models be used for enterprise mobility? & SRQ2: Which process steps should be taken to assess mobile risks and how should these steps be executed?

Traditional risk management processes, standards and models provided a solid base to the introduced M-RAM artifact. By comparing industry standard risk assessment processes a reference method (Levantakis, Helms & Spruit, 2008) was determined. This process was then crafted to a risk assessment process that is suitable for an assessment on mobility. The introduced method to the M-RAM approach provides clear guidance on how to execute the mobile risk assessment. This approach is evaluated and validated by a real-life case study, which makes the approach very suitable to execute in business environments. Concluded, it can be stated that traditional risk management processes provide a solid base for mobile risk management processes. Still, the translation to a ‘mobile’ approach is key to conduct a successful mobile risk assessment.

SRQ3: Which entities are involved with enterprise mobility and how are these involved?

The final M-RAM approach includes four different involved entities. The first two involved entities 'Enterprise Organization' and 'Employees' are internal entities that are obvious, but very important to consider as employees can pose serious threats. The other two involved entities 'Business Partners' and Potential harmdoers' are entities that externally threaten the assessed organization. The 'Business Partners' group involves all entities that have a business relation with the assessed organization (E.g. clients, suppliers and consultants) and are able to (mis) use the enterprise mobile services of the assessed organization. The second group 'Potential harmdoers' is the most complex and dangerous group as it involves anyone that does not have a formal relation with the assessed organization but can harm the organization by misusing the enterprise mobile services of the assessed organization. An intentional harmful entity can be anyone that deliberately tries to harm the assessed organization financially, reputation wise or in other manners. The unintentional harmful entities (E.g. employee's relatives and finders of lost devices) are often underestimated, but can also form a great threat to the organization. Concluding it is very important to consider the four different entity groups during the mobile risk assessment, in order to understand the threats and vulnerabilities that originate from the different entities.

SRQ4: How can mobile vulnerabilities and mitigating controls be identified and categorized?

Based on the Systematic Literature Review, the 22 expert interviews and existing risk assessment frameworks, eight different mobile attention areas are determined during this research. The final eight attention areas are areas that can contain vulnerabilities as well as mitigating controls related to enterprise mobility. The identification of vulnerabilities can be done using three techniques, (1) consider how determined threats can be opposed, (2) consider a list of general mobile vulnerabilities and (3) consider possible vulnerabilities in each of the eight attention areas. The identification of mitigating controls can be done using three similar techniques, (1) consider how determined vulnerabilities are mitigated, (2) consider a list of general mitigating controls and (3) consider possible mitigating controls in each of the eight attention areas. The case study in this research validated that the M-RAM assessor should be able to categorize each vulnerability or control in one of the eight attention areas. Concluding, the eight different attention areas provide the ability to categorize vulnerabilities and controls, but more important the areas help to identify vulnerabilities as well as controls during the mobile risk assessment.

RQ: How can one assess the risks that originate from the usage of enterprise mobility within enterprise organizations?

The introduction of the M-RAM approach and method aims to answer the main research question. Risks that originate from enterprise mobility can be assessed using the risk assessment process that is based on industry accepted risk assessment processes and adapted for mobile risk assessments. Furthermore, the risk assessment process is complemented with knowledge about involved entities with enterprise mobility and mobile attention areas, in order to determine mobile vulnerabilities and controls. The M-RAM approach and method is based on extensive literature research and the knowledge of 22 mobile security & risk experts. Moreover, the M-RAM approach and method are validated using a case study in an organization with extensive mobile usage and very sensitive information.

General Conclusions and Discussion

This section discusses and concludes general findings that are related to the field of enterprise mobility, mobile security and mobile risk management. The findings are based on the literature review, expert interviews and the main researcher's insight during the research project.

"Maturity in mobile management varies widely"

Although no mobile management maturity model was used and no concrete definition of mobile maturity is mentioned, the 22 interviewed mobile security experts provided a clear variety in the maturity in mobile management of enterprise organizations. Some organizations are still catching up with the fast introduction and acceptation of mobile devices within the company, where others already defined different mobile management processes, strategies and risk management frameworks.

"BYOD is not really happening!"

BYOD is a huge trend that really was hyped in 2013. However, none of the interviewed mobile security managers has indicated that their organization supported a BYOD program. Different models as restricted BYOD (Employees can bring some supported devices) or CYOD (Choose your device from a list of supported devices) are supported, but the actual BYOD model is not really happening. Furthermore, mobile managers indicate that BYOD will probably never be realized within their organizations, as it is simply unmanageable due the enormous variation of operating system versions and mobile devices. Concluding, it can be stated that BYOD within Dutch enterprise organizations is not happening at the moment.

"MDM is a tool, not a solution"

Mobile Device Management tools are used by most of the interviewed enterprise organizations to enforce policies, set security controls and monitor mobile usage. However, organizations often consider their MDM tool as the solution to mobile security and mobile risk management. The controls that organizations install are often based on the capabilities of their MDM solution, not considering the actual threats and vulnerabilities that are posed to the organization. MDM is a tool to realize determined controls that should be based on a risk assessment and not a complete solution to mobile security and risk management.

"Organizations think in controls, not in risks"

The main remark derived from several expert interviews and the different case study workshops is that people in the field of mobile management and mobile security mainly think in controls rather than thinking in risks or threats. People find it really hard to determine the 'initial' threats to an organization, when controls are already in place. This limitation often complicates the practice of determining threats to an organization. Therefore, people need to change their mindset when conducting the mobile risk assessment method in order to identify the real threats that are opposed to the organization.

8.3 Future Work

The M-RAM artifact and method is validated by using a real-life case study at a company that was very suitable for conducting the M-RAM method. Still, the environment and context of other organizations can vary from the case study environment. Therefore, the first future work opportunity is to conduct case studies in environments that vary from the case study of this research, in order to generalize the method. Deloitte, the sponsoring company of this research, is very likely to adopt this method in their risk advisory services. This would directly result in multiple cases where the method will be validated.

During the research of this study, multiple problems and research questions arose that were not in scope of this research, but are highly related to this research. First, there were multiple discussions with mobile security experts on how devices like hybrid laptops (PCMag, 2013) will evolve in the coming years and how they will or will not integrate with notebooks. The main question from a security perspective was how organizations should deal with mobile security, should mobile devices be treated differently from conventional computers or should they be treated the same. A possible research question for this future research could be: *How is security management of mobile devices different from conventional computers?*

Secondly, different mobile security experts as well as stakeholders in the conducted case study indicated that it is really hard to deal with the enormous release pace of new mobile devices, mobile operating systems and especially MDM systems. Organizations are struggling with implementing new versions of devices and software as they are not able to oversee functional as well as security consequences. Moreover, employees are expecting to benefit from new devices and operating system immediately. This leads in the behavior where employees are ignoring policies by updating to new software versions before the organization supports it. A possible research question for this future research could be: *How should enterprise organizations manage and release new versions of mobile devices, operating systems and mobile device management software?*

The last future research opportunity is related to the trend of Bring Your Own Device (BYOD). Surprisingly, almost all 22 interviewed mobile security experts indicate that BYOD is not really happening, mainly because the variety in devices and operating systems is unmanageable. Furthermore, the mobile security experts state that the model of distributing and managing mobile devices really depends on the type of organization and mobile usage. However, it remains unclear how organizations should decide which distribution and management model they should use for mobile devices. A great research opportunity is to develop a framework that helps organizations in deciding which mobile distribution and management model they should use. A possible research question for this future research could be: *How should organizations decide which distribution and management model they should use for mobile devices?*

Enterprise mobility is a very interesting research field that will likely grow in the near future. Conducting the proposed future research will help organizations in professionalizing their mobile usage and it will help employees in getting the most out of mobility.

9 References

Air-Watch (2013). Enabling Bring Your Own Device (BYOD) In the Enterprise. Retrieved August, 2013. From http://www.airwatch.com/resources/

Alberts, C., & Dorofee, A. (2001). An Introduction to the OCTAVESM Method. white paper, CERT, http://www.cert.org/octave/methodintro.html.

Anvaari, M., & Jansen, S. (2010, August). Evaluating architectural openness in mobile software platforms. In Proceedings of the Fourth European Conference on Software Architecture: Companion Volume (pp. 85-92). ACM.

Aroms, E. (2012). NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems.

Aroms, E. (2012). NIST Special Publication 800-39 Managing Information Security Risk.

Arxan (2012) State of Security in the App Economy: "Mobile Apps Under Attack". Re-trieved August 2013. From http://www.arxan.com/resources/state-of-security-in-the-app-economy/

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011, May). Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In Security and Privacy (SP), 2011 IEEE Symposium on (pp. 96-111). IEEE.

Bensberg, F. (2009). Mobile Business Intelligence. In Erfolgsfaktoren des Mobile Marketing (pp. 71-87). Springer Berlin Heidelberg.

Bickford, J., O'Hare, R., Baliga, A., Ganapathy, V., & Iftode, L. (2010, February). Rootkits on smart phones: attacks, implications and opportunities. In Proceedings of the eleventh workshop on mobile computing systems & applications (pp. 49-54). ACM.

Bloemendal, W. E. (2012). App stores for owners: a multiple-case study of app stores.

Brinkkemper, S., van de Weerd, I., Saeki, M., & Versendaal, J. (2008). Process improvement in requirements management: A method engineering approach. In Requirements Engineering: Foundation for Software Quality (pp. 6-22). Springer Berlin Heidelberg.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing octave allegro: Improving the information security risk assessment process (No. CMU/SEI-2007-TR-012). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Cavaye, A. L. (1996). Case study research: a multi‐faceted research approach for IS. Information systems journal, 6(3), 227-242.

CERT (2013). Computer Emergency Response Team. Retrieved August 2013, from http://www.cert.org/octave/

Chen, C. L., Lee, C. C., & Hsu, C. Y. (2012). Mobile device integration of a fingerprint biometric remote authentication scheme. International Journal of Communication Systems, 25(5), 585-597.

Chen, I. J., & Popovich, K. (2003). Understanding customer relationship management (CRM): People, process and technology. Business Process Management Journal, 9(5), 672-688.

CBP (2013) College Bescherming Peroonsgegevens. Retrieved August, 2013. from http://www.cbpweb.nl/Pages/home.aspx

Cisco (2012) BYOD: A Global Perspective. Retrieved August, 2013. From http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global_Top10-Insights.pdf
Codenomicon (2010). Unknown Vulnerability Management. Retrieved August, 2013. From http://www.codenomicon.com/resources/whitepapers/codenomicon-wp-unknown-vulnerability-management.pdf

COSO (2004) Executive summary of Enterprise Risk Management – Integrated Framework. Retrieved August, 2013 from http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf

COSO (2012) Enterprise Risk Management for Cloud Computing. Retrieved August 2013, from http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf

COSO (2013) Committee of sponsoring organizations of the treadway commission. Retrieved August 2013, from http://www.coso.org/default.htm

Crawford, H., Renaud, K., & Storer, T. (2013). A Framework for Continuous, Transparent Mobile Device Authentication. Computers & Security.

Curkovic, S., Scannell, T., Wagner, B., & Vitek, M. (2013). A Longitudinal Study of Supply Chain Risk Management Relative to COSO's Enterprise Risk Management Framework. Modern Management Science & Engineering, 1(1), p13.

Dagon, D., Martin, T., & Starner, T. (2004). Mobile phones as computing devices: The viruses are coming!. Pervasive Computing, IEEE, 3(4), 11-15.

Davis, A., Nowak, G., & Vrhovec, G. (2011). Securing consumer devices. Information Security Forum.

Derballa, V., & Pousttchi, K. (2004, March). Extending knowledge management to mobile workplaces. In Proceedings of the 6th international conference on Electronic commerce (pp. 583-590). ACM.

Duff, A. (1996). The literature search: a library-based model for information skills instruction. *Library Review, 45, 14-18.*

Enck, W., Gilbert, P., Chun, B. G., Cox, L. P., Jung, J., McDaniel, P., & Sheth, A. (2010, October). TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. In OSDI (Vol. 10, pp. 255-270).

Ferraiolo, D. F., & Kuhn, D. R. (2009). Role-based access controls. arXiv preprint arXiv:0903.2171.

Forbes. (2013). *Is the market ready for a Phablet ?, Retrieved July, 2013, from* http://www.forbes.com/sites/rogerkay/2012/02/07/is-the-market-ready-for-a-phablet/

Forrester (2013). Benchmarking Mobile Engagement: Consumers And Employees Outpace CIOs' Readiness. Retrieved, August 2013. From http://www.forrester.com/Benchmarking+Mobile+Engagement+Consumers+And+Employees+Outpace+CIOs+Readiness/fulltext/-/E-RES95601

Godwin-Jones, R. (2011). Emerging technologies: Mobile apps for language learning. *Language Learning & Technology*, *15*(2), 2-11.

Gorman, M., & Carlson, B. (1989). Can experiments be used to study science?. Social Epistemology, 3(2), 89-106.

Greamo, C., & Ghosh, A. (2011). Sandboxing and virtualization: Modern tools for combating malware. Security & Privacy, IEEE, 9(2), 79-82.

Jacobsen, D. I., & Hellstorm, C. (2002). Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämne. Lund: Studentlitteratur.

Harris, J., Ives, B., & Junglas, I. (2012). IT consumerization: when gadgets turn into enterprise IT tools. MIS Quarterly Executive, 11(3), 99-111.

Harris, M. A., Patten, K., & Regan, E. (2013). The Need for BYOD Mobile Device Security Awareness and Training.

Hart, C. (2001). Doing a literature search: a comprehensive guide for the social sciences. Sage.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS quarterly, 28(1), 75-105.

Hoog, A. (2011). Android forensics: investigation, analysis and mobile security for Google Android. Access Online via Elsevier.

Hornyack, P., Han, S., Jung, J., Schechter, S., & Wetherall, D. (2011, October). These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. In Proceedings of the 18th ACM conference on Computer and communications security (pp. 639-652). ACM.

Howe, A. E., & Dreilinger, D. (1997). SAVVYSEARCH: A metasearch engine that learns which search engines to query. AI Magazine, 18(2), 19.

Hyrynsalmi, S., Mäkilä, T., Järvi, A., Suominen, A., Seppänen, M., & Knuutila, T. (2012). App store, marketplace, play! an analysis of multi-homing in mobile software ecosystems. In Proceedings of the International Workshop on Software Ecosystems (p. 59).

IDC (2013). Smartphone Operating System Highlights. Retrieved July 2013, from http://www.idc.com/getdoc.jsp?containerId=prUS24108913

Idu, A., van de Zande, T., Jansen, S.: Multi-homing in the Apple ecosystem: Why and how developers target multiple Apple App Stores. In: Proceedings of the International Conference on Management of Emergent Digital EcoSystems. MEDES '11, New York, NY, USA, ACM (2011) 122{128

ISACA (2009). The Risk IT Framework. Retrieved August 2013, from http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx

ISACA (2013). Trust in, and value from, information systems. Retrieved August 2013, from https://www.isaca.org/Pages/default.aspx

ISF (2013). Information Security Forum. Retrieved August 2013, from https://www.securityforum.org/membership/

IMore (2013). iOS 7 preview: new security features. Retrieved July 2013, from http://www.imore.com/new-security-features-coming-ios-7

ISO/IEC 27005, (2008). ISO/IEC 27005:2008 , Information security risk management. Geneva, Switzerland: ISO/IEC.

ISO/IEC 27000, (2009). ISO/IEC 27000: Information security management systems — Overview and vocabulary. Geneva, Switzerland: ISO/IEC.

ISO/IEC 31000, (2009). ISO/IEC 31000: Risk management — Principles and guidelines Geneva, Switzerland: ISO/IEC.

ISO (2013). International Organization for Standardization. Retrieved August 2013, from http://www.iso.org/iso/home.htm

Jansen, S., & Bloemendal, E. (2013). Defining App Stores: The Role of Curated Marketplaces in Software Ecosystems. In Software Business. From Physical Products to Software Services and Solutions (pp. 195-206). Springer Berlin Heidelberg.

Keyes, J. (2013). Bring Your Own Devices (BYOD) Survival Guide. CRC Press.

Leavitt, N. (2011). Mobile security: Finally a serious problem?. Computer, 44(6), 11-14.

Lerotic, S. (2012). Distributing Applications in 2012.

Levantakis, T., Helms, R., & Spruit, M. (2008). Developing a reference method for knowledge auditing. In Practical Aspects of Knowledge Management (pp. 147-159). Springer Berlin Heidelberg.

Lin, H. F. (2011). An empirical investigation of mobile banking adoption: the effect of innovation attributes and knowledge-based trust. International Journal of Information Management, 31(3), 252-260.

Louise Barriball, K., & While, A. (1994). Collecting Data using a semi-structured interview: a discussion paper. Journal of advanced nursing, 19(2), 328-335.

Lookout (2012). State of mobile security. Retrieved July 2013, from https://www.lookout.com/resources/reports/state-of-mobile-security-2012

MaaS360 (2013). Does Android dream of Enterprise adoption? Retrieved August 2013, from http://content.maas360.com/www/content/wp/wp_maas360_mdm_androidDream.pdf

Mandujano, S. (2013). Privacy in the Mobile Hardware Space: Threats and Design Considerations.

Microsoft. (2013). *Which Surface is right for you?* Retrieved July 2013, from http://www.microsoft.com/surface/en-us/which-surface-is-right-for-you

Miller, C. (2011). Mobile attacks and defense. Security & Privacy, IEEE, 9(4), 68-70.

Miller, C., Blazakis, D., DaiZovi, D., Esser, S., Iozzo, V., & Weinmann, R. P. (2012). iOS hacker's handbook. Wiley. com.

Mitroff, I. I., & Featheringham, T. R. (1974). On systemic problem solving and the error of the third kind. Behavioral Science, 19(6), 383-393.

Mobiquity (2013). Mobile Security Begins with Risk Management. Retrieved July 2013, from http://www.mobiquityinc.com/files/whitepapers/Mobiquity%20White%20Paper%20%7C%20Risk%20Management.pdf

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. Network Security, 2012(12), 5-8.

National Cyber Security Centrum. (2012) Beveiligingsrichtlijnen voor mobiele apparaten. Retreived July 2013, from https://www.ncsc.nl/dienstverlening/expertiseadvies/kennisdeling/whitepapers/beveiligingsrichtlijnen-voor-mobiele-apparaten.html

Negrino, T. (2013). iCloud: Visual QuickStart Guide. Peachpit Press.

Niehaves, B., Köffer, S., & Ortbach, K. (2012). IT Consumerization–A Theory and Practice Review.

NIST (2013). National Institute of Standards and Technology. Retrieved August 2013, from http://www.nist.gov/index.html

Oberheide, J., & Jahanian, F. (2010, February). When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments. In Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications (pp. 43-48). ACM.

Paavilainen, J. (2002). Mobile business strategies: understanding the technologies and opportunities. Pearson Education.

PCMag. (2013). Definition of: hybrid laptop. Retrieved July, 2013, from http://www.pcmag.com/encyclopedia/term/63893/hybrid-laptop

Perkins, J. (2013). London School of Economics. Information Security: Information Classification. Retrieved August 2013, from http://www.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/infSecStaIT.pdf

Petticrew, M., Roberts, H., & MyiLibrary. (2006). Systematic reviews in the social sciences: A practical guide. MA: Blackwell Pub.

Rasmussen, N. H., Bansal, M., & Chen, C. Y. (2009). Business dashboards: a visual catalog for design and deployment. Wiley.

Redman, Phillip, John Girard, and Basso Monica. "Magic quadrant for mobile device management software." Gartner Research (2012).

Rhee, K., Jeon, W., & Won, D. (2012). Security Requirements of a Mobile Device Management System. International Journal of Security and Its Applications, 6, 353-358.

Rouse, M. (2012). *Enterprise app store.* Retrieved July, 2013, from http://searchconsumerization.techtarget.com/definition/enterprise-app-store-enterprise-application-store

Ruebsamen, T., & Reich, C. (2012, July). Enhancing mobile device security by security level integration in a cloud proxy. In CLOUD COMPUTING 2012, The Third International Conference on Cloud Computing, GRIDs, and Virtualization (pp. 159-168).

Symantec (2012). Exploiting the business potential of BYOD . Retrieved July, 2013. from http://www.symantec.com/zh/tw/content/en/us/enterprise/white_papers/b-byod-exploiting-bus-potential-wp-21256109-en.us.pdf

Schadler, T., & McCarthy, J. C. (2012). Mobile Is The New Face Of Engagement. Forrester Research, February, 13.

Seriot, N. (2010). iPhone privacy. Black Hat DC, 30.
Shim, J. P., Mittleman, D., Welke, R., French, A. M., & Guo, J. C. (2013). Bring Your Own Device (BYOD): Current Status, Issues, and Future Directions.

Simon, H. A. (1996). The sciences of the artificial. MIT press.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267-270.

Souppaya, M., Scarfone, K., (2013). Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST Special Publication 800-124 Revision 1.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five.

Sybase (2013). Mobility Advantage: Why Secure Mobile Devices? Retrieved August, 2013. From http://www.sybase.nl/files/White_Papers/Sybase_Afaria_WhySecurity_wp.pdf

Tarasewich, P., Nickerson, R. C., & Warkentin, M. (2002). Issues in mobile e-commerce. Communications of the association for information systems, 8(1), 41-64.

Tenable Network Security (2012). Mobile Device Vulnerability Management Flagged as Top Concern for Security Professionals in 2012. Retrieved August, 2013. From www.tenable.com/news-events/press-releases/2012-mobile-devicevulnerability-management-flagged-astop-concern-for-se.

Trustwave (2013). Keep calm and bring your own. Retrieved July, 2013. From https://www.trustwave.com/downloads/whitepapers/Trustwave_WP_BYODSecurity_2013.pdf

Vaishnavi, V., & Kuechler, W. (2004). Design research in information systems.

Vaishnavi, V. K., & Kuechler Jr, W. (2007). Design science research methods and patterns: innovating information and communication technology. CRC Press.

Verkooij, K. (2012). Mobile Business Intelligence.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly, 26(2), 13-23.

Weinmann, R. P. (2012, August). Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks. In WOOT (pp. 12-21).

Wessel, S., Stumpf, F., Herdt, I., & Eckert, C. (2013). Improving Mobile Device Security with Operating System-Level Virtualization. In Security and Privacy Protection in Information Processing Systems (pp. 148-161). Springer Berlin Heidelberg.

Wood, P., Nisbet, M., Egan, G., Johnston, N., Haley, K., Krishnappa, B., & Hittel, S. (2012). Symantec internet security threat report trends for 2011. Volume XVII.

Wu, I. L., Li, J. Y., & Fu, C. Y. (2011). The adoption of mobile healthcare by hospital's professionals: an integrative perspective. Decision Support Systems, 51(3), 587-596.

Xia, R., Rost, M., Holmquist, L.E.: Business models in the mobile ecosystem.
In: Ninth International Conference on Mobile Business and 2010 Ninth Global
Mobility Roundtable. ICMB-GMR (2010) 1/8

Xu, Q., Erman, J., Gerber, A., Mao, Z., Pang, J., & Venkataraman, S. (2011, November). Identifying diverse usage behaviors of smartphone apps. In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference (pp. 329-344). ACM.
Yin, R. K. (2009). Case study research: Design and methods. CA: Sage Publications.

Zenprise (2013). The shift to MDM 2.0. Retrieved July, 2013. From
http://wavelink.com.au/downloads/zenprise/The_Shift_to_MDM_2.0.pdf

10 Appendices

Appendix A – Interview protocols

Mobile Security Expert

Mobile security specialists that consult organizations on mobile security or on mobile security products (MDM). The specialists need to have knowledge about existing threats, vulnerabilities, risks, but also the mitigating actions that need to be in place.

1. What is your current position/role?
2. What is your background regarding mobile security?
    - Education?
    - Projects?
    - Technologies?
    - Experience?

Demand & Usage

3. If you look at the current market, what do organizations want to achieve with the use of mobility? Can you rank this on importance?
4. If you look at the current market, how are mobile devices often…
    - Provided?
    - Used?
    - Supported?
5. Do you think organizations often postpone mobile innovation because mobile security & governance is to complex and not mature enough? Do you see a clear tension field between innovation & security?
6. What is the best way to measure/monitor which devices/apps/data that is used by which user (groups)?

Threats

7. What are, in your opinion, the most important threats for organizations that are caused by mobility? Can you rank these on importance?
8. In your opinion, which of these threats should get more attention from organization?
9. What is the best way to identify and classify threats? Is this also done in practice?
10. Does it often occur that threats become reality? If so, what is mostly the cause and was this to be prevented?
11. Are there any typical threats that organizations don't realize?

Vulnerabilities

12. Mobility causes vulnerabilities in different attention areas like device or user level. Can you categorize these vulnerabilities in different attention areas?
13. How should you identify vulnerabilities in each category/attention area?
14. Which vulnerabilities are the most difficult to identify?
15. Are there vulnerabilities that are often not recognized by organizations?

Risk & impact

16. What is the best way to do a mobility risk assessment based on the identified threats and vulnerabilities?

Mitigation actions

17. If you should identify mitigating actions, would you use the same categorization as with vulnerabilities? If not, what would be different?
18. How should you identify mitigating actions that are already taken for each category?
19. Should you relate mitigating actions directly to threats, risks or vulnerabilities?
20. What are, in your opinion, the most important governance and security steps that you need to take when introducing a BYOD program?

Risk evaluation

21. How often should you reassess risks? Should this been done when introducing new functionality or by using regular intervals?

Wind-up

22. How do you see mobile security developing in the coming year?
23. Do you see any upcoming changes in security caused by the fact that laptops and tablets are becoming more and more the same or hybrid in other words?
24. What do you think about concept M-RAM (reference) method? Would you change anything?
25. Are there any aspects regarding mobile security that are not mentioned?
26. Do you know persons in your environment that know a lot of this subject and may be willing to support me in my research?

Mobile Security Manager

Information Risk managers within enterprise organizations that are responsible for threats, vulnerabilities and risks that originate form Enterprise Mobility.

1. What is your current position/role?
2. What is your background regarding mobile security?
    - Education?
    - Projects?
    - Technologies?
    - Experience?

Demand & Usage

3. What does your organization want to achieve with the use of Enterprise Mobility? Can you rank this on importance
4. How are mobile devices (smartphones, tablets)…
    - Provided?
    - Used?
    - Supported?
5. Which mobile solutions on app level are implemented or are on the agenda to be implemented?
6. Which mobile solutions are desirable but not yet implemented or on the agenda? Can you rank these on importance?
7. Do you see a clear tension field between mobile innovation & security? Are mobile innovations often postponed or declined due security reasons?
8. Does the organization take the wish of their employees in account?
9. Are there any measurement/monitoring applications used to check which devices/os are used?
10. Are there any measurement/monitoring applications used to check which apps are used?
11. Are there any measurement/monitoring applications used to check which and how information is used?

Threats

12. What threats caused by enterprise mobility do you concern? Can you rank then on importance?
13. In your opinion, which of these threats should get more attention?
14. How do you identify and classify threats?
15. Does it often occur that threats become reality? If so, what is mostly the cause and was this to be prevented?

Risk & impact

16. Are mobile risks calculated, if so, how are they calculated?

Mitigation controls

17. Are mitigating controls always related to threats, vulnerabilities or risks?
18. What are in your opinion the most important governance and security steps that you need to take when introducing a BYOD program?

19. Do you use a MDM system? If so, to what extent does it solve your security and governance problems?

Risk evaluation

20. Are risks re-evaluated when mitigating controls are applied? And are the residual risks than formally accepted?
21. How often should you reassess risks? Should this been done when introducing new functionality or by using regular intervals?

Wind-up

22. How do you see mobile security developing in the coming year?
23. Do you see any upcoming changes in security caused by the fact that laptops and tablets are becoming more and more the same or hybrid in other words?
24. Are there any aspects regarding mobile security that are not mentioned?
25. Do you know persons in you environment that know a lot of this subject and may be willing to support me in my research?

Appendix B – Mobile profile

	Supported by organization	Actual mobile environment
Business activities supported by mobile		
Devices		
OS		
Apps		
Device ownership		
Payment (device & plan)		

Appendix C – Information assets

Information asset	Sort	Classification
E-mail	On device	Restricted
ERP	Accessed by device	Restricted

Appendix D – Mobile assets

Manufacturer	OS version	Known vulnerabilities	Key controls	Classification
Apple	iOS5			Trusted
Apple	iOS6			Trusted
Apple	iOS7			Trusted

Appendix E – Guidelines for threats, vulnerabilities & controls

This appendix provides threats, vulnerability and control guidelines from different sources that are used as a starting point for the case study validation described in section 7 Validation. Some of the guidelines are in Dutch as they are provided in Dutch by the guideline source.

Threat guidelines

Threat	Area	Source
Unintentional leaking of data from apps	Apps	NCSC
Use of untrusted applications	Apps	NIST 800-124
Corporate data access unavailability	Data & Network	Deloitte
Data leakage through insecure data storage	Data & Network	Deloitte
Data leakage through unauthorised/ insecure/ malicious application	Data & Network	Deloitte
Eavesdropping or modifying network traffic	Data & Network	NCSC
Interaction with other systems (e.g. sync with untrusted home computer)	Data & Network	NIST 800-124
Leaking of data	Data & Network	NCSC
Unauthorised access to internal network	Data & Network	Deloitte
Use of Location Services (attacker can determine where the device is)	Data & Network	NIST 800-124
Use of untrusted networks	Data & Network	NIST 800-124
Diallerware (stealing money by SMS and phone services)	Device	NCSC
Lack of physical security	Device	NIST 800-124
Spyware	Device	NCSC

Surveiliance (following of targeted user)	Device	NCSC
Use of untrusted devices	Device	NIST 800-124
Insufficient OS version control	MDM platform	Deloitte
Financial malware	Users	NCSC
Phishing	Users	NCSC
Rogue devices & Identity theft	Users	Deloitte
Use of untrusted content	Users	NIST 800-124

Vulnerability guidelines

Vulnerability	Area	Source
Zwakke authenticatiemechanismen bij appdistributie	Apps	NCSC
Unauthorized and unapproved installation of applications by end users; control is challenging	Apps	Deloitte
Third party application vulnerabilities, applications with questionable motives	Apps	Deloitte
Lack of “mobile-ready” support and operational processes, infrastructure	Control processes	Deloitte
Lack of resources, skill sets and technical capabilities in-house	Control processes	Deloitte
Zwakheden in de toegepaste encryptiemethode voor gegevensopslag	Data & Network	NCSC
Onveilige gegevensopslag	Data & Network	NCSC
Onveilige of onvoldoende beveiligde netwerkverbinding	Data & Network	NCSC
Kwetsbaarheden waardoor malware geïnstalleerd kan worden	Data & Network	NCSC
Kwetsbaarheden in reputatiesystemen	Data & Network	NCSC
Data on removable media	Data & Network	MaaS360
Kwetsbaarheden in het mobiele besturingssysteem of de geïnstalleerde apps	Devices	NCSC
Lack of native encryption on devices, memory cards and at the OS level (for certain Operating Systems	Devices	Deloitte
Lack of drive encryption	Devices	MaaS360
Rooting posibility	Devices	MaaS360
Zwakke sandboxing implementatie	MDM platform	NCSC
Highly diverse mobile ecosystem due to multiple mobile Operating Systems and carrier specific implementations	MDM platform	Deloitte
Lack of mobile OS patching and update enforcement	MDM platform	Deloitte

End users modifying device security controls, bypassing corporate controls	MDM platform	Deloitte
Remote wipe not a panacea — attempts frequently fail for lost and stolen mobile devices	MDM platform	Deloitte
Er zijn geen privacy 'best practices' beschikbaar	Privacy & Compliance	NCSC
Potential privacy issues due to personnel activity, device use, data exposure, etc.	Privacy & Compliance	Deloitte
Ethical and legal questions around monitoring, device wiping, securing devices and data upon employee termination, etc.	Privacy & Compliance	Deloitte
Regulatory requirements regarding e-discovery, monitoring, data archiving need to be considered	Privacy & Compliance	Deloitte
Verlies of diefstal van het mobiele apparaat	Users	NCSC
Op onjuiste manier buiten gebruik stellen van het mobiele apparaat	Users	NCSC
Gebrek aan bewustwording bij gebruikers	Users	NCSC
Gebrek aan vaardigheid bij gebruikers	Users	NCSC
Moeilijk (lastig) voor gebruiker om inzicht te krijgen in vereiste (en toegekende) gebruikersrechten	Users	NCSC
End users (including corporate executives) are increasingly driving decisions around devices	Users	Deloitte

Control guidelines

Guideline	Attention Area	Source
Restrict which app stores may be used.	Apps	NIST 800-124
Restrict which applications may be installed through whitelisting (preferable) or blacklisting.	Apps	NIST 800-124
Restrict the permissions (e.g., camera access, location access) assigned to each application.	Apps	NIST 800-124
Install, update, and remove applications. Safeguard the mechanisms used to perform these actions. Keep a current inventory of all applications installed on each device.	Apps	NIST 800-124
Restrict the use of operating system and application synchronization services (e.g., local device synchronization, remote synchronization services and websites).	Apps	NIST 800-124
Verify digital signatures on applications to ensure that only applications from trusted entities are installed on the device and that code has not been modified.	Apps	NIST 800-124
Distribute the organization's applications from a dedicated mobile application store.	Apps	NIST 800-124

Het aantal geïnstalleerde apps dient te worden beperkt	Apps	NCSC
Installeer alleen apps op het moment dat bekend is wie deze app heeft gemaakt en de maker van deze app wordt vertrouwd	Apps	NCSC
Beperk de rechten van geïnstalleerde apps tot een absoluut minimum	Apps	NCSC
Configureer de browser zodanig dat het noodzakelijke beveiligingsniveau wordt gegarandeerd	Apps	NCSC
Voorzie tijdig alle software van de laatste versies/patches	Apps	NCSC
Locatievoorzieningen dienen zoveel mogelijk te zijn uitgeschakeld	Apps	NCSC
Het mobiele apparaat dient 'schoon' in te worden geleverd	Apps	NCSC
Installeer alleen apps als de bron bekend is	Apps	NCSC
Schakel JavaScript uit	Apps	NCSC
Schakel fraudemeldingen in	Apps	NCSC
Schakel automatisch vullen van webformulieren uit	Apps	NCSC
Schakel Privémodus (Incognitomodus) in	Apps	NCSC
Schakel cookies accepteren uit	Apps	NCSC
Schakel beveiligingswaarschuwingen weergeven in	Apps	NCSC
Information flow enforcement (information flows should be controlled by an authorized person)	Control processes	NIST 800-53
Remote access (remote access to information assets should be controlled and monitored)	Data & Network	NIST 800-53
Wireless access (wireless network management)	Data & Network	NIST 800-53
Access control for mobile devices (limit access when users are using mobile devices compared to traditional devices)	Data & Network	NIST 800-53
Strongly encrypt data communications between the mobile device and the organization. This is most often in the form of a VPN, although it can be established through other uses of secure protocols and encryption.	Data & Network	NIST 800-124
Strongly encrypt stored data on both built-in storage and removable media storage. Removable media can also be "bound" to particular devices such that encrypted information can only be decrypted when the removable media is attached to the device, thereby mitigating the risk of offline attacks on the media.	Data & Network	NIST 800-124
Wipe the device (to scrub its stored data) before reissuing it to another user, retiring the device, etc.	Data & Network	NIST 800-124
Remotely wipe the device (to scrub its stored data) if it is suspected that the device has been lost, stolen, or otherwise fallen into untrusted hands and is at risk of having its data recovered by an untrusted party.	Data & Network	
A device often can also be configured to wipe itself after a certain number of incorrect authentication attempts.	Data & Network	NIST 800-124
Versleutel opgeslagen gegevens waar mogelijk	Data & Network	NCSC
Versleutel verzonden gegevens waar mogelijk	Data & Network	NCSC

Schakel netwerkverbindingen zoveel mogelijk uit wanneer deze niet worden gebruikt	Data & Network	NCSC
Schakel de mobiele internetverbinding (mobiele data) uit als hier geen gebruik van wordt gemaakt	Data & Network	NCSC
Schakel dataroaming uit als hier geen gebruik van wordt gemaakt	Data & Network	NCSC
Schakel Persoonlijke hotspot uit als hier geen gebruik van wordt gemaakt	Data & Network	NCSC
Schakel Wi-Fi uit als hier geen gebruik van wordt gemaakt	Data & Network	NCSC
Stel het mobiele apparaat zo in dat Wi-Fi-netwerken, waar eerder verbinding mee is gemaakt, worden vergeten	Data & Network	NCSC
Stel het mobiele apparaat zo in dat er niet wordt gevraagd om een verbinding te maken met een Wi-Fi-netwerk	Data & Network	NCSC
Stel het mobiele apparaat zo in dat er niet automatisch met een Wi-Fi-netwerk wordt verbonden	Data & Network	NCSC
Maak zoveel mogelijk gebruik van een VPN-verbinding	Data & Network	NCSC
Schakel Bluetooth uit als hier geen gebruik van wordt gemaakt	Data & Network	NCSC
Schakel Near Field Communication (NFC) uit als hier geen gebruik van wordt gemaakt	Data & Network	NCSC
Schakel vliegtuigmodus in13, 14, 15 als geen draadloze netwerkverbindingen en voorzieningen nodig zijn	Data & Network	NCSC
User identification and authentication (on device)	Devices	NIST 800-53
Device identification and authentication (known, trusted device)	Devices	NIST 800-53
Require a device password/passcode and/or other authentication (e.g., token-based authentication, network-based device authentication, domain authentication) before accessing the organization's resources. This includes basic parameters for password strength and a limit on the number of retries permitted without negative consequences (e.g., locking out the account, wiping the device).	Devices	NIST 800-124
If device account lockout is enabled or the device password/passcode is forgotten, an administrator can reset this remotely to restore access to the device.	Devices	NIST 800-124
Have the device automatically lock itself after it is idle for a period (e.g., 5 minutes).	Devices	NIST 800-124
Under the direction of an administrator, remotely lock the device if it is suspected that the device has been left in an unlocked state in an unsecured location.	Devices	NIST 800-124
Jailbreak of root nooit het mobiele apparaat	Devices	NCSC
Schakel de functies die ondersteuning bieden bij het ontwikkelen van apps - zoals USB foutopsporing uit	Devices	NCSC
Maak gebruik van verschillende toegangscodes voor het mobiele apparaat, de verschillende diensten en apps	Devices / MDM platform	NCSC
Wijzig regelmatig de toegangscode van het mobiele apparaat, de verschillende diensten en apps	Devices / MDM platform	NCSC

Stel een toegangscode in om het mobiele apparaat te ontgrendelen	Devices / MDM platform	NCSC
Stel een toegangscode in om het mobiele apparaat te ontgrendelen die bestaat uit een combinatie van alfabetische, numerieke en niet-alfanumerieke tekens	Devices / MDM platform	NCSC
Stel het maximaal aantal toegestane mislukte aanmeldingspogingen in	Devices / MDM platform	NCSC
Schakel SIM-kaartvergrendeling in	Devices / MDM platform	NCSC
Stel automatische vergrendeling in waardoor het mobiele apparaat na een bepaalde periode wordt vergrendeld	Devices / MDM platform	NCSC
Sta apps niet toe om de gecodeerde opslag van certificaten, toegangscodes en andere credentials te benaderen.	Devices / MDM platform	NCSC
Schakel het tonen van de toegangscode tijdens het invoeren uit	Devices / MDM platform	NCSC
Schakel voorvertoning van berichten (voor Android alleen SMS-berichten) op het beginscherm uit	Devices / MDM platform	NCSC
Access enforcement (enforce a proper access way)	MDM platform	NIST 800-53
Configuration settings (Manage device settings	MDM platform	NIST 800-53
Restrict user and application access to hardware, such as the digital camera, GPS, Bluetooth interface, USB interface, and removable storage.	MDM platform	NIST 800-124
Restrict user and application access to native OS services, such as the built-in web browser, email client, calendaring, contacts, application installation services, etc.	MDM platform	NIST 800-124
Manage wireless network interfaces (Wi-Fi, Bluetooth, etc.)	MDM platform	NIST 800-124
Automatically monitor, detect, and report when policy violations occur, such as changes from the approved security configuration baseline, and automatically take action when possible and appropriate	MDM platform	NIST 800-124
Maak gebruik van volgsoftware (MDM)	MDM platform	NCSC
Managing Users (providing different access levels to users)	MDM platform	MaaS360
Upgrade and Patch management	MDM platform	MaaS360
Minimum OS version enforcement	MDM platform	MaaS360
White - black listing of apps	MDM platform	MaaS360
Media sanitization (device wiping)	MDM platform / Devices	NIST 800-53
Er dient inzichtelijk te zijn welke privacygevoelige en vertrouwelijke gegevens worden verwerkt	Privacy & Compliance	NCSC
Er dienen maatregelen genomen te worden die de privacygevoelige en vertrouwelijke gegevens afdoende beschermen	Privacy & Compliance	NCSC
Er dienen maatregelen genomen te worden die gebruikers bewust en bekwaam maken	User	NCSC
Security Awareness training / programs	Users	NIST 800-53
Audit events	Users	NIST 800-53

Appendix F – Threat classification

Threat	C	I	A
Hacking	x	x	
Denial of Service attack			x

Appendix G – Threat Vulnerability Analysis

No	Threat	No	Vulnerability	Area
1	Hacking	1	No drive encryption	Device
		2	Get around passcode	Device
		3	Unsecured WiFi allowed	Data & Network
2	Denial of Service attack	4	MDM IP publically available	MDM Platform

Appendix H – Risk quantification

No	Trigger	Threats	Likelihood	Impact		Risk
1	External	Theft	4	5		**20**
2	Internal	Loss	4	5		**20**

Appendix I – Risk – Control relation

No	Threats (Risk)	No	Mitigating control	Attention Area
1	Theft	1	VPN, certificates, user/password	Data & Network
		2	Encryption	Devices
		3	Device policy (MDM)	MDM platform
		4	General awareness mail	Users
		5	Wipe control (MDM)	MDM platform

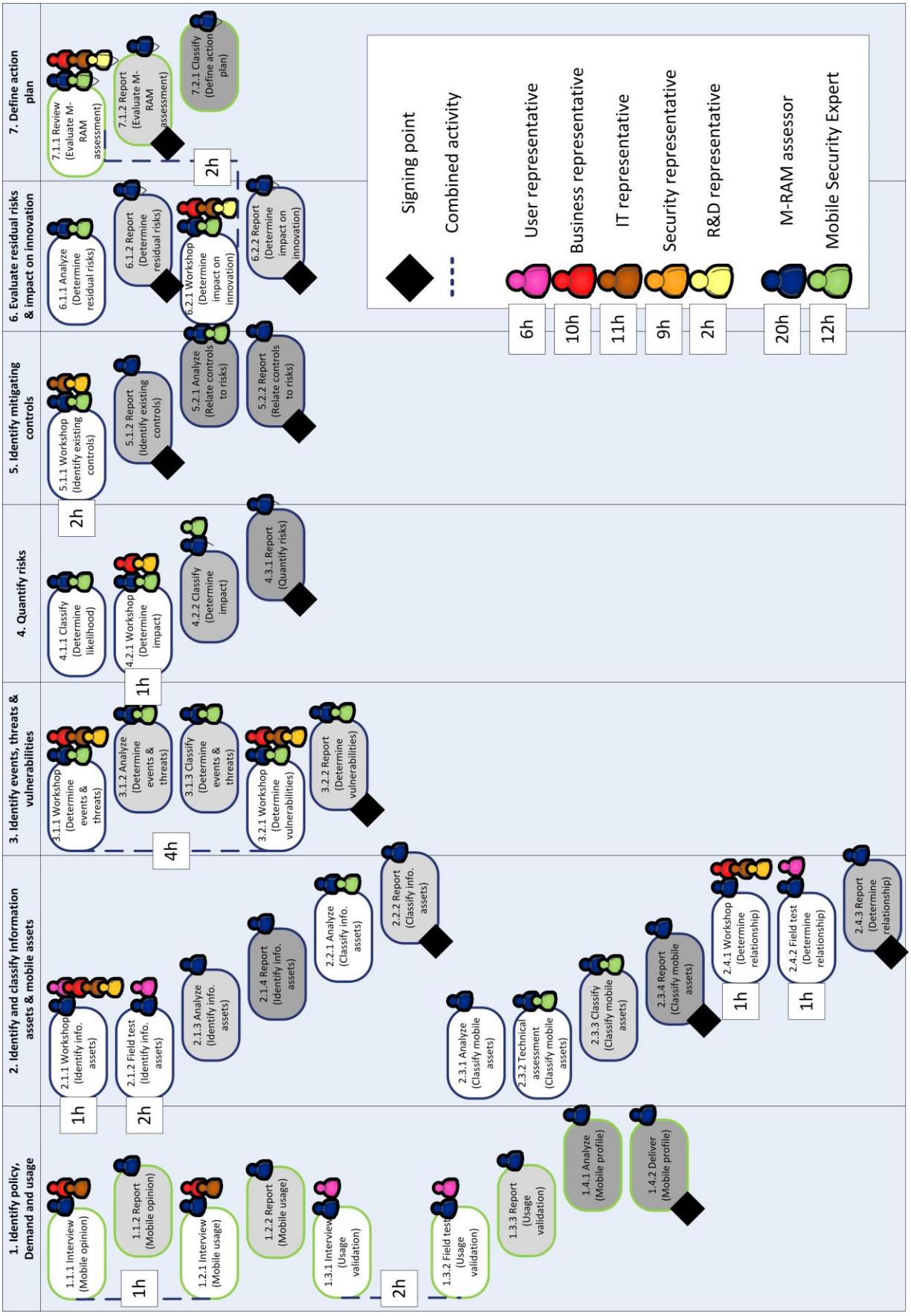
Appendix J – Residual risk

No	Threats	Like-lihood	Impact	Initial Risk		Residual Like-lihood	Residual Impact	Residual Risk
1	Theft	4	5	**20**		4	1	**4**
2	Loss	4	5	**20**		4	1	**4**

Appendix K – Impact on Innovation

Innovation theme	Influencing controls	Impact
BYOD	1, 2, 5	2
BYOA	6,7	3
Customized apps	1,5,7	4
Usability	4	1

Appendix L – M-RAM work program



Appendix M – Case study results

Phase 1: Mobile opinion

As output of step 1.1.2 (Report) the mobile opinion of the case company is reported, which is determined by interviewing four different people in the organization from business, IT and security departments. The interview data is merged and interpreted in order to answer the following questions;

- What does your organization want to achieve with the use of Enterprise Mobility?

The main goal is to allow employees in working location and time independent. Furthermore, we are more and more working on solutions that will allow employees to support and execute primary processes by the use of mobile devices.

- Is enterprise mobility a strategic asset or an infrastructure part for your organization?

Enterprise mobility is not yet a strategic asset of the organization, but this will change in the near future when mobile devices are used to support our primary process. Mobile devices are certainly part of our infrastructure and used extensively.

- Are mobile devices used for supportive processes, primary processes or both?

It really depends on the user and what you consider primary. In general it can be stated that mobile devices are mostly used to support primary as well as supportive processes. The execution of primary processes by using mobile devices will likely be done in the future.

Phase 1: Mobile usage

As output of step 1.2.2 (Report) the mobile usage of the case company is reported, which is determined by interviewing four different people in the organization from business, IT and security departments. The interview data is merged and interpreted in order to answer the following questions;

- How are mobile devices (smartphones and tablets) supplied and who is paying for the device and carrier contract?

Business managers decide which employees are eligible for a mobile device and which mobile device. The manager can than order a mobile device from a web portal that contains of devices that are approved and supported by the IT supplier. The business manager pays for the device and its monthly subscription & support costs.

When the device is delivered, the IT department makes a physical appointment with the user and the user has to prepare itself by creating an Apple-id if necessary. Next, IT support together with the user will install the MDM (MobileIron) app and a VPN connection app. After that the MDM will push the predefined configuration to the mobile device and the user is ready to go.

- Are users allowed to bring their own device for business purposes and connect to the organization's network?

No, users are never allowed to bring and use their own device. It is also not possible to connect a non-registered device to the corporate network. For guest, a one-day WiFi code can be generated with username, password and shared-key security.

- Can you provide a list of (approved) business activities (including: mail, agenda, contacts, web portals, document sharing, chat, people finder, supportive and primary applications) that are executed on mobile devices?

Applications are not white or blacklisted, which means that the user can install any app. Furthermore, three apps are developed and a list of recommended apps exist (This list will later be evaluated).

- Is application management enforced or are there guidelines for which applications may be used and which not?

All applications are allowed and there is thus no application management. However, users are triggered and guided to use apps in an appropriate way.

- Who is responsible for mobile business and mobile security?

The business decides on mobile usage and initiatives. When new functionality is desired, the business determines the functional requirements and hands them over to the IT and other supportive departments. Often it is unclear what the exact requirements are and more alignment between business need and mobile delivery is needed.

Phase 1: Usage validation

As output of step 1.3.3 (Report) the mobile usage of the case company is validated by field tests. Different users are asked on their mobile usage and their devices are inspected to validate earlier statements about mobile usage. The collected data is merged and interpreted in order to validate mobile usage.

Device & function

User 1: iPad 3, supportive function
User 2: iPad 3, supportive function
User 3: iPad 2 & BB, primary function

Questions

- How does the organization provide mobile devices and who is paying for the device and the carrier contract?

User 1: Manager decides that I needed an iPad, and then the device was ordered. The organization pays for the iPad and I don't have a subscription for a 3G connection.
User 2: I heard that I was getting an iPad from my manager. The organization pays for the device, but not for a 3G subscription (in my position).
User 3: Governance board decided to use iPads and ordered them. The organization fully pays the device and there are no additional cost for me as a user.

- How did you receive your device?

User 1: I received a mail that my device was delivered and when I needed to pick up the device at the WPO (workplace support) desk
User 2: First I was asked to create an Apple-id in advance, then I was informed by WPO that my device was delivered and when I could pick up the device. I needed to sign a device agreement and several certificates, and management apps (MobileIron, Junos Pulse) were installed at the WPO desk.

User 3: I had to pick up the device at a local servicepoint of WPO (workplace support), their the device was installed and I was informed on how to use the device.

- What do you use your mobile device for (Applications, processes, tasks)?

User 1: Mostly for games, multimedia and other private applications. For business purposes I only use mail and the 'notes' app during meetings.
User 2: The organization provides some business apps like the people finder app or an app that explains how you should work digital. Still, I only use e-mail, notes and a radio app in my daily work. To be honest my children mostly use the iPad by playing games or watching movies. I mostly use the iPad for mailing and browsing when I am at home.
User 3: I use the device for many activities in my daily work, at first my E-mail. Documents on meetings and cases are often sent over mail. I mostly store the documents using Dropbox or bluefire and then read them on my iPad. It would be create to access dossiers on the iPad, but this is not possible yet.

**Note: corporate appstore and the people finder app does not seem the work during the field test of User 2*

Field test

User 1:
Device and OS: *iPad 3, iOS 6.1.3*
Device owner: *Organization*
Installed (business) apps: *tba, different social media, gaming and multimedia apps*
Device Management: *MobileIron, complicated password identified*

User 2:
Device and OS: *iPad 3, iOS 6.1.3*
Device owner: *Organization*
Installed (business) apps: *Business:* Figure 47: Business apps, user 2 *Private: different social media, gaming and multimedia apps*
Device Management: *MobileIron, multiple certificates, complicated password identified*

Figure 47: Business apps, user 2

User 3:
Device and OS: *iPad 3, iOS 6.1.3*
Device owner: *Organization*
Installed (business) apps: *Bluefire, Dropbox, different public business apps*
Device Management: *MobileIron, complicated password identified*

Phase 2: Information assets

As output of step 2.1.4 and 2.2.2 (Report) the identified information assets are listed and classified. Based on the interviews and field test from phase 1 and the organized workshop in step 2.1.1 the different information assets that are stored and accessed by a device are identified. The workshop had an unexpected twist as all participants agreed that every enterprise information asset can technically be accessed on every enterprise iOS device. Therefor a summarized list of information assets is made to avoid a never ending list of information assets (Table 8: Information Asset Classification).

Information asset	Sort	Classification
E-mail	On device	Restricted, confidential
SharePoint documents	On device	Restricted, confidential
Internal network drive documents	On device	Restricted, confidential
All documents that can be accessed and stored via any web service	On device	Restricted, confidential
SharePoint team sites (when credentials)	Accessed by device	Restricted, confidential
Any web application	Accessed by device	Restricted, confidential
Remote desktop to any server (when credentials)	Accessed by device	Restricted, confidential

Table 8: Information Asset Classification

Phase 2: Device Assets

As output of step 2.3.4 (Report) the identified device assets and its properties are listed and classified. Based on the interviews and field test from phase 1, and the technical assessment (workshop) in step 2.3.2, the different device assets that are used by the organization are identified. Table 9: Device Asset Classification provides an overview of the device (security) characteristics and how the devices are classified in different trust levels.

	iPhone	iPad	BlackBerry	Android/ Windows
Devices	4S, 5	2, 3, 4, Mini	Different devices	Not supported
Operating system	iOS 6.1.3*	iOS 6.1.3*	Different versions	-
Management	MobileIron	MobileIron	BES Server	-
Device access	5 digit code (changed every two months)	>8 character password ** (changed every two months)	>8 character password ** (changed every two months)	-
Encryption	Standard Apple encryption	Standard Apple encryption	Standard BB encryption	-
Connection	VPN, ActiveSync	VPN, ActiveSync	BES Server	-
Remote control	Wipe, lock, Location, Message, Monitoring	Wipe, lock, Location, Message, Monitoring	Standard BES functionality	-
Authentication	Username/password, certificates	Username/password, certificates	Username/password, BES	-

OS trust level	High	High	High	Low
Not supported				x
Basic security				
Managed	x	x	x	
Trusted				

Table 9: Device Asset Classification

*Users need to update their device to the latest supported version (iOS 6.1.3) but are not technically shutdown when they don't.
**Three out of the four defined password complexity rules need to be addressed.

Phase 2: Relation between devices and information assets

As output of step 2.4.3 (Report) the relation between the identified device assets and the identified information asset is defined by explaining which information is used on which device. The classification is based on the output of the information asset classification; the device asset classification and the workshop were the relation between assets is determined. Table 10: Asset relationships' shows the relation between the classified devices and classified information assets.

	Confidential	Restricted	Internal Use	Public
Trusted	x	x	x	x
Managed	x	x	x	x
Basic				x
Not supported				x

Table 10: Asset relationships

Phase 3: Threats

As output of step 3.1.3 (Classify) the threats that are identified during the workshop of step 3.1.1 are listed and classified on confidentiality (C), integrity (I) and availability (A). Table 11: Threat identification & classification provides an overview of the determined threats and their impact on confidentiality (C), integrity (I) and availability (A).

No	Trigger	Threats	C	I	A
1	External	Theft	X		X
2	Internal	Loss	X		X
3	External	Eavesdropping	X		
4	Internal / external	Data leakage (conscious)	X		
5	Internal / external	Data leakage (unconscious)	X		
6	External	Identity theft		X	
7	External	Black mail	X	X	
8	External	Fraud		X	
9	Internal	Lacking user awareness	X	X	
10	Internal	Deliberately ignoring policy	X	X	
11	Internal	Regulation		X	
12	Internal / external	Business continuity			X
13	External	Infiltration	X	X	
14	External	Unauthorized access	X	X	
15	Internal	Human error	X	X	
16	Internal	Privacy violation		X	
17	Internal	Losing usability			X

Table 11: Threat identification & classification

Phase 3: Threats and vulnerabilities

As output of step 3.2.2 (Report) the identified threats of step 3.1.3 are linked to the identified vulnerabilities in step 3.2.1 (workshop). The vulnerabilities that are linked to the identified threats make it possible to realize (expose) the threat. Table 12: Threats and linked vulnerabilities' shows how each vulnerability is linked to the identified threats.

No	Threats	No	Vulnerability	Attention Area
1	Theft	1	Lack of physical security	Environment
		2	Popular good	Environment
		3	Location (device is everywhere)	Environment
		4	Carelessness of employees	Users
		5	Lacking user awareness	Users
2	Loss	1	Lack of physical security	Environment
		2	Popular good	Environment
		3	Location (device is everywhere)	Environment
		4	Carelessness of employees	Users
		5	Lacking user awareness	Users
3	Eavesdropping	6	Unconscious of possibility	Users
		7	Usage in public locations	Environment
4	Data leakage (conscious)	8	24/7 possibility of leaking data	Environment
		9	Easy to link data to private environment	Data & Network
		10	Data is stored on device	Data & Network
5	Data leakage (unconscious)	11	Human error	Users
		12	Access to relatives	Environment
		13	Access to app and cloud suppliers	Apps
		5	Lacking user awareness	
6	Identity theft	14	Unlocked device	Device
		15	Inadequate enrolment/out of service process	Control processes
		5	Lacking user awareness	
7	Blackmail / fraud	16	Inadequate behaviour of employees	Users
		17	Unsatisfied employees	Users
8	Deliberately ignoring policy	18	Missing functionality	Users
		19	Convenience	Users
		20	Power, acting exempt from policy	Users
		21	Overkill in security controls	Users
9	Violating regulation	22	(International) unknown regulations	Privacy & compliance
10	Business continuity disruption	23	Inadequate IT management	Control processes
11	Infiltration	24	Inadequate device access management	MDM platform
		25	Inadequate usage monitoring	MDM platform
12	Unauthorized	24	Inadequate device access	MDM platform

	access		management	
		25	Inadequate usage monitoring	MDM platform
		15	Inadequate enrolment/out of service process	Control processes
13	Privacy violation	27	Location services	Privacy & compliance
		28	Wiping device with private content	Privacy & compliance

Table 12: Threats and linked vulnerabilities

Phase 4: Risk quantification

As output of step 4.3.1 (Report) the identified threats of step 3.1.3 are quantified on likelihood and impact. Both the likelihood and impact are classified on a scale from 1 (low) to 5 (high). Furthermore, the 5 impact values can be translated to economical loss as described in the work program. Table 13: Risk quantification provides an overview of the quantified risks.

Low risk	1-5
Medium risk	6-15
High risk	16-25

No	Trigger	Threats	Likelihood	Impact		Risk
1	External	Theft	4	5		**20**
2	Internal	Loss	4	5		**20**
3	External	Eavesdropping (shoulder serving)	3	3		**9**
4	Internal / external	Data leakage (conscious)	3	5		**15**
5	Internal / external	Data leakage (unconscious)	4	5		**20**
6	External	Identity theft	2	5		**10**
7	External	Blackmail / fraud	1	5		**5**
8	Internal	Deliberately ignoring policy	5	5		**25**
9	Internal	Regulation	1	3		**3**
10	Internal / external	Business continuity	2	4		**8**
11	External	Infiltration	3	5		**15**
12	External	Unauthorized access	5	5		**25**
13	Internal	Privacy violation	4	5		**20**

Table 13: Risk quantification

Phase 5: Mitigating controls

As output of step 5.1.2 (Report) and 5.2.2 (Report) the identified controls are listed and related to the earlier identified threats. Each control is categorized to the attention areas of the M-RAM artifact. Table 14: Mitigating controls provides an overview of the identified controls.

No	Threats	No	Mitigating control	Attention Area
1	Theft	1	VPN, certificates, user/password	Data & Network
		2	Encryption	Devices
		3	Device policy (MDM)	MDM platform
		4	General awareness mail	Users
		5	Wipe control (MDM)	MDM platform
2	Loss	1	VPN, certificates, user/password	Data & Network
		2	Encryption	Devices
		3	Device policy (MDM)	MDM platform
		4	General awareness mail	Users
		5	Wipe control (MDM)	MDM platform
3	Eavesdropping		**No controls**	
4	Data leakage (conscious)	4	General awareness mail	Users
		6	Provide alternative to cloud apps	Apps
		7	Incident response process	Control processes
5	Data leakage (unconscious)	4	General awareness mail	Users
		6	Provide alternative to cloud apps	Apps
		7	Incident response process	Control processes
6	Identity theft	1	VPN, certificates, user/password	Data & Network
		2	Encryption	Devices
		3	Device policy (MDM)	MDM platform
		4	General awareness mail	Users
		5	Wipe control (MDM)	MDM platform
7	Black mail / Fraud		**No controls**	
8	Deliberately ignoring policy	3	Device policy (MDM)	MDM platform
		4	General awareness mail	Users
		5	Wipe control (MDM)	MDM platform
		6	Provide alternative to cloud apps	Apps
9	Violating regulation		**No controls**	
10	Business continuity disruption		**No controls**	
11	Infiltration	3	Device policy (MDM)	MDM platform
		4	General awareness mail	Users
		5	Wipe control (MDM)	MDM platform
		8	Device (issue) control processes	Control processes
12	Unauthorized access	1	VPN, certificates, user/password	Data & Network
		3	Device policy (MDM)	MDM platform
		4	General awareness mail	Users
13	Privacy violation	9	Access to user's location limited to administrators	Privacy & compliance

Table 14: Mitigating controls

Phase 6: Residual risk

As output of step 6.1.2 (Report) the residual likelihood, impact and risk to each threat is determined. Both the likelihood and impact are again classified on a scale from 1 (low) to 5 (high. Table 15: Residual risks provides a list of the residual risks.

Low risk	1-5
Medium risk	6-15
High risk	16-25

No	Threats	Like-lihood	Impact	Initial Risk	Residual Like-lihood	Residual Impact	Residual Risk
1	Theft	4	5	**20**	4	1	**4**
2	Loss	4	5	**20**	4	1	**4**
3	Eavesdropping (shoulder serving)	3	3	**9**	3	3	**9**
4	Data leakage (conscious)	3	5	**15**	2	5	**10**
5	Data leakage (unconscious)	4	5	**20**	3	5	**15**
6	Identity theft	2	5	**10**	1	5	**5**
7	Blackmail / fraud	1	5	**5**	1	5	**5**
8	Deliberately ignoring policy	5	5	**25**	5	5	**25**
9	Regulation	1	3	**3**	1	3	**3**
10	Business continuity	2	4	**8**	2	4	**8**
11	Infiltration	3	5	**15**	1	5	**5**
12	Unauthorized access	5	5	**25**	5	5	**25**
13	Privacy violation	4	5	**20**	3	5	**15**

Table 15: Residual risks

Phase 6: Impact on innovation

As output of step 6.2.1 (Report) controls that constrain innovation and usability are listed. The workshop group also evaluated the impact on innovation and usability by estimating the amount of impact using a scale from 1 (low) till 5 (high).

Innovation / usability theme	Influencing controls	Impact
Password policy (iPhone)	3	3 (Medium)
Password policy (iPad)	3	5 (High)
Screen lock out time (iPad)	3	5 (High)
No BYOD allowed	1, 8	1 (Low)
No primary process support	8	4 (High)

Table 16: Impact on innovation & usability

Informal statements:

During the different workshops, interviews and assessment a lot of statements regarding mobile security are made. These statements are not directly used in the M-RAM assessment, but can be of value to the organization. Therefore an anonymous quote list is defined.

"I use the iPad in my daily work, case documents or links internal stored documents are often shared over mail. I then store these documents on Dropbox and access them during meetings." (Business)

"When new mobile OS updates are released, it is only tested whether functional aspects are still working. New versions are not tested on security vulnerabilities." (Security)

Appendix N – Final M-RAM method (work program)