Delft University of Technology

A BYOD Enterprise Security Architecture for accessing SaaS cloud services

Vasileios Samaras

4187377

Master Thesis

A BYOD Enterprise Security Architecture for accessing SaaS cloud services

MASTER THESIS
Submitted in partial fulfillment of the requirements for the degree of
Master of Science in Management of Technology

Author : Vasileios Samaras
Student number : 4187377

Graduation Committee:
Chairman: Prof. Dr. ir. Jan van den Berg
Professor, Section Information and Communication Technology

First supervisor: Dr. ir. Semir Daskapan
Assistant Professor, Section Information and Communication Technology

Second supervisor: Dr. ir. Floor Koornneef
Associate Professor, Section Safety Science Group

Third supervisor: Dr. ir. Laurens Rook
Assistant Professor, Section Technology, Strategy and Entrepreneurship

MSc Program Management of Technology
Faculty of Technology, Policy and Management
Delft University of Technology, the Netherlands

Abstract

In contemporary times IT plays a major role in enterprises' business processes. Companies pursue the adoption of new technological trends in order to improve their business in terms of both performance and efficiency so that they can keep up with the fierce market competition. However, the introduc tion of cloud computing services and the opportunity for employees to work using their own smart phones through the adoption of BYOD/BYOS policies introduce additional risk for the firms' processes. The question that needs to be answered is how the aforementioned risks can be reduced to acceptable levels, in order to support a secure adoption of IT consumerization and SaaS cloud computing trends. In order to answer this question, this report proposes a component security architecture for enterprises. The design of it is based on a desk research on academic and industrial literature, by which the enterprise environment is defined. Additional hardware, software and service-oriented security components are applied, using the SABSA security architecture framework, in order to secure the SaaS cloud services access by Smartphone BYOD.

Keywords

SABSA security architecture, Smartphone, BYOD, BYOS, Cloud sprawl, Mobile device management

Acknowledgements

I would like to extend my genuine gratitude to the following persons who were involved in this Thesis research:

My First Supervisor, dr. Semir Daskapan, for giving me the opportunity to look into this intriguing and challenging topic and for his invaluable guidance and feedback throughout the process that led me to gain genuine interest in the Information Security field.

The Chairman of my Thesis committee, Prof. dr. Jan van den Berg, and my Second Supervisor, dr. Floor Koornneef for their support, invaluable insights and patience in assisting me to complete this research.

All the academic and industry experts for the time they took to provide their insights on my research findings, through which they contributed in validating the design results.

Finally, I would like to express my love and gratitude to my family and friends for their unconditional support throughout the two years of this Master's programme.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

3G	Third Generation
4G	Fourth Generation
ACL	Access Control List
AES	Advanced Encryption Standard
BRP	Business Risk Profile
BYOD	Bring Your Own Device
BYOS	Bring Your Own Software
CDMA	Code Division Multiple Access
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
DAC	Discretionary Access Control
DES	Data Encryption Standard
DiDI	Defense in Depth Index
DMZ	Demilitarized Zone
DoS	Denial of Service
DPA	Data Protection Act
E2AF	Extended Enterprise Architecture Framework
EU	European Union
FIPS	Federal Information Processing Standards
GDPR	General Data Protection Regulation
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HBI	High Business Impact
HR	Human Resources
HRM	Human Resources Management
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
LBI	Low Business Impact
LOB	Line Of Business
MAC	Mandatory Access Control
MBI	Medium Business Impact
MDM	Mobile Device Management
MitM	Man-in-the-Middle
NIST	National Institute of Standards & Technology
OS	Operating System
PaaS	Platform as a Service
PIN	Personal Identification Number
RBAC	Role-based Access Control
SaaS	Software as a Service
SABSA	Sherwood Applied Business Security Architecture
SCM	Supply Chain Management
SLA	Service Level Agreement
SOMF	Service-Oriented Modeling Framework
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WPA	Wi-Fi Protected Access

Chapter 1: Introduction

1.1 Defining the scope of the research

Security is a very broad term that can be broken down to a number of concepts, depending on the type of the system that has to be secured. In the IT realm, five quality attributes compose a system's security: confidentiality, integrity, availability, access control and non-repudiation (66). This report looks into the security architectures that firms incorporate in their overall business architecture to secure the access of cloud services by employee-owned smart phones. An enterprise security architecture comprises the design artifact that explains how to position and interrelate a number of security controls, in order to maintain the aforementioned quality attributes (13), (14).

Cloud computing is a newly introduced technology defined as the on-demand network access to a shared pool of computing resources, such as storage, applications, networks and servers for software development and deployment. These resources are customizable and can be rapidly provisioned and released with less management effort than maintaining the infrastructure on premises (9). The opportunities that cloud computing can offer are practically unlimited; still they can be categorized in the following three service models: "Software as a Service" (SaaS), "Platform as a Service" (PaaS) and "Infrastructure as a Service" (IaaS). In the SaaS model users utilize specific applications (e.g. online office suites, file sharing applications) that are organized on a single logical environment on the SaaS cloud (2). The PaaS model offers a development platform where both completed and in-progress cloud applications are hosted. App developers may utilize the tools provided by the PaaS vendor to program their own software, whereas end-users can execute the various completed apps on the cloud. Finally, in the IaaS model users can rent IT infrastructures that are provided on the IaaS cloud (5), (6).

As cloud computing becomes more widespread, many enterprises adopt cloud solutions in their businesses, due to the benefits offered. With cloud computing companies do not have to bear the heavy up-front costs for IT hardware and software (1). On the contrary, they have the option of renting the services from an external cloud provider, who guarantees their availability and secure operation, provides technical support and ensures constant software updates (7). As an enterprise may grow successfully, cloud solutions offer much more flexibility thanks to the per-user service offering than a traditional in-house solution that would require purchasing of new hardware and hiring/training of more employees, which is more costly and time consuming (8).

Nevertheless, a downside of cloud services is that each cloud model raises different security issues for the enterprise (9). The reason for this is that due to the enterprise owning a "slice" of the cloud space in cases of IaaS and PaaS clouds, it maintains more control on the virtual space, in contrast to SaaS clouds, where different enterprises share the same environment, which is controlled by the SaaS vendor (6), (8). This

tradeoff of offering more freedom in building applications on a dedicated cloud space extends to security features and capabilities, where the built-in capabilities are less complete, but there is more flexibility to layer on additional security components (2), (1). In the SaaS model the cloud provider is responsible for managing and securing all aspects of the network, server and application infrastructure. However, in PaaS clouds enterprises are responsible for access control to the applications, whereas in the IaaS model the firm is entirely responsible for managing all security aspects of their resources in the cloud. The research of this report is limited to SaaS cloud adoption, where control over the cloud environment lies on the provider's side; consequently, the enterprise security responsibilities are limited to applying on-premises controls and securing the delivery endpoints (19).

Cloud computing is only one part of the IT consumerization trend that opens up new possibilities for innovation in enterprise mobility. Another new technology force that is related to enterprise mobility is the "Bring your own Device" (BYOD) trend. Instead of the company providing the required hardware/software to its employees, by adopting BYOD policies, individual employees can choose and often own the computers or smart phones they use at work (2). Since they are already familiar with how to use these devices, they can work more productively (11). Apart from higher work satisfaction, BYOD policies shift costs to the user, which enhances cost-efficiency for the firms (10). In addition, employee-owned devices can help enterprises become more innovative, since these devices tend to be more cutting edge. Consequently organizations can reap the benefits of the features and capabilities that the latest smart devices have to offer (3).

The current trend of more and more powerful mobile devices has shifted the computing market from personal computers to smart phones (22). In this sense, personal smart phones have come to resemble general-purpose computers (23). More specifically, smart phones are simply computers with an additional GSM (Global System for Mobile Communications) radio and a baseband processor that controls it (20). Smartphone manufacturers are pushing their mobile device technology so hard that today's smart phone power can be equivalent to low-end personal computers, but with lower cost and better portability. The superiority of smart phones indicates that the smart phone market is going to increase even faster in the following years (22). Consequently, smart phones are now increasingly being used as gateways to the enterprise information infrastructure (21). Not only do smart phones provide anywhere, anytime access, they come equipped with multiple onboard sensors, high-end processors, rich storage resources and different network capabilities, which can assist in context sensitive retrieval of information (21), (22).

1.2 Problem statement

Despite the benefits offered, smart phones represent a particular risk. Since smart phone technology is still relatively new, the vendors' security approaches are still not mature enough (24). What is more, the increasing number of open mobile platforms that

customers could choose from makes smart phones more vulnerable to hackers and malware (25). A critical issue at stake is the "Bring your own Software" (BYOS) issue, which is defined as the employees' unregulated use of public SaaS applications with an aim to process corporate data. This new threat, known as Cloud Sprawl, derives from the evolution of the SaaS delivery endpoint from a fixed enterprise workstation to smart phones (2). Whereas firms make great efforts to enforce security on the on-premise hardware, off-the-shelf personal devices lack specific enterprise configurations (4), (17). Organizations have very little visibility into the endpoint itself, while employees are left responsible for securing their own smart phones (18). In this sense, employee ownership markedly constrains the security capabilities that can be deployed on the phones (21). Forbidding Smartphone BYOD is not an effective solution, due to the fact that employees will still pursue to use their smart phones in the enterprise. Rather than baring a higher risk due to lacking any oversight on the employee owned devices, it is preferred for enterprises to implement a BYOD enterprise information security architecture, which constitutes of a number of technical components that, along with organizational and physical controls, can secure the employee use of personal smart phones for business purposes. Such a security architecture does not exist in the current context.

That said the adoption of Smartphone BYOD policies for processing corporate data through SaaS applications is not problem-free (2). As a result, the issue at the core of this research can be defined as follows:

"Current enterprise information security architectures do not provide a tailored security solution for accessing SaaS cloud services by BYOD"

1.3 Research objective and research questions

Considering the importance of information technologies in business processes and the unlimited opportunities that Smartphone BYOD policies and cloud computing technologies open up for new and existing firms, it is clear that there is an uprising trend of mobility policy adoption in all business sectors. Since the main drawback for companies is the lack of robust security policies that will guarantee the firm's safe operation, the importance of analyzing and redesigning an enterprise security architecture, considering the threats related to the adoption of cloud computing and IT consumerization trends is more evident than ever. Moreover, due to the consequential expansion of stakeholder network, it is deemed necessary that all parties' interests and needs are taken into account. As a result, the main objective of this research is to propose:

"An enterprise information security architecture that treats the information security risks induced by Smartphone BYOD accessing SaaS cloud services".

By approaching the aforementioned objective from a business perspective, the main research question that can resolve the issue at stake is described as follows:

Q0: "What enterprise information security architecture can secure the access of SaaS cloud services by Smartphone BYOD?

The system at stake consists of the enterprise itself and the external cloud that provides the SaaS services. Within the company, the stakeholders involved are the employees and the management board that share different views and interests. The rest of the stakeholder network in such a system comprises the customers that are renting services from the enterprise, the external cloud vendor, the mobile network operators and the Smartphone vendors that relate to the employee Smartphone usage. Governmental authorities are also involved through data protection legislations that the enterprise should comply with. In order to answer the main research question, our research is broken down into the following sub-questions that are analyzed throughout this report:

Q1: "What are the relevant business processes that take place amongst the different stakeholders involved in the enterprise-cloud system?"

Q2: "What is the underlying IT infrastructure in the enterprise-cloud system?"

Q3: "What are the main design requirements that the proposed security architecture needs to fulfill?"

Q4: "Based on a risk assessment, which security risks can be identified when enterprises combine SaaS services with Smartphone integration policies"

Q5: "What are the components that constitute the proposed security architecture?"

Q6: "How can the validity of the proposed architecture be established?"

In order to accomplish the research objective of designing an enterprise information security architecture it is crucial that the above sub-questions are sequentially addressed. Consequently, the first step of the research is to gain thorough understanding of the processes that take place amongst the different parties involved in the system at stake. The next step is to define the underlying IT infrastructure of the enterprise-cloud system as well as the communication channels between the different components. Since the main goal is to resolve the issues deriving from accessing SaaS cloud services by Smartphone BYOD, upon defining the context and the technologies implemented in the enterprise-cloud system, the security and legal requirements that the security architecture has to meet are defined. Next, a risk assessment is performed in order to identify the key information risks for the firm's most valuable assets. Based on the outcome of the risk evaluation and the definition of design requirements, a set of security components is proposed and their precise integration in the enterprise-cloud environment constitutes the proposed security architecture. Finally, the sixth sub-question aims to check the validity and viability of the proposed security architecture by conducting interviews with security experts.

1.4 Research methodologies

1.4.1 Methodology selection and research assumptions

This research relates to the Design Science Research paradigm, and is therefore based on the Information Systems Research framework proposed by Hevner et al., as illustrated in Figure 1 below (9). The organizational problem at stake is that the adoption of mobility policies and SaaS clouds raises security issues for the enterprises' business processes. Since consumerization trends become more popular, due to their flexibility and cost reduction benefits, it is crucial that the enterprise security architecture is redesigned, in order to resolve the issues at stake. Before describing how the Information Systems Research framework is applied to our research, we need to elaborate on the assumptions made prior to our research. As already discussed, our research is limited to SaaS cloud adoption, due to the reduced complexity for enterprises adopting this type of clouds, since the cloud vendor is responsible for securing the SaaS cloud environment. Another restriction in our research is that we only take into account the use of smart phones as the BYOD endpoint, since these devices are nowadays the prominent hardware and therefore require the most attention by enterprises considering mobility policies. Finally, the proposed architecture's applicability is restricted for enterprises within the European Union, due to a large diversity in the cultural, legal and business environments outside the EU boundaries that can affect the security architecture's design requirements.

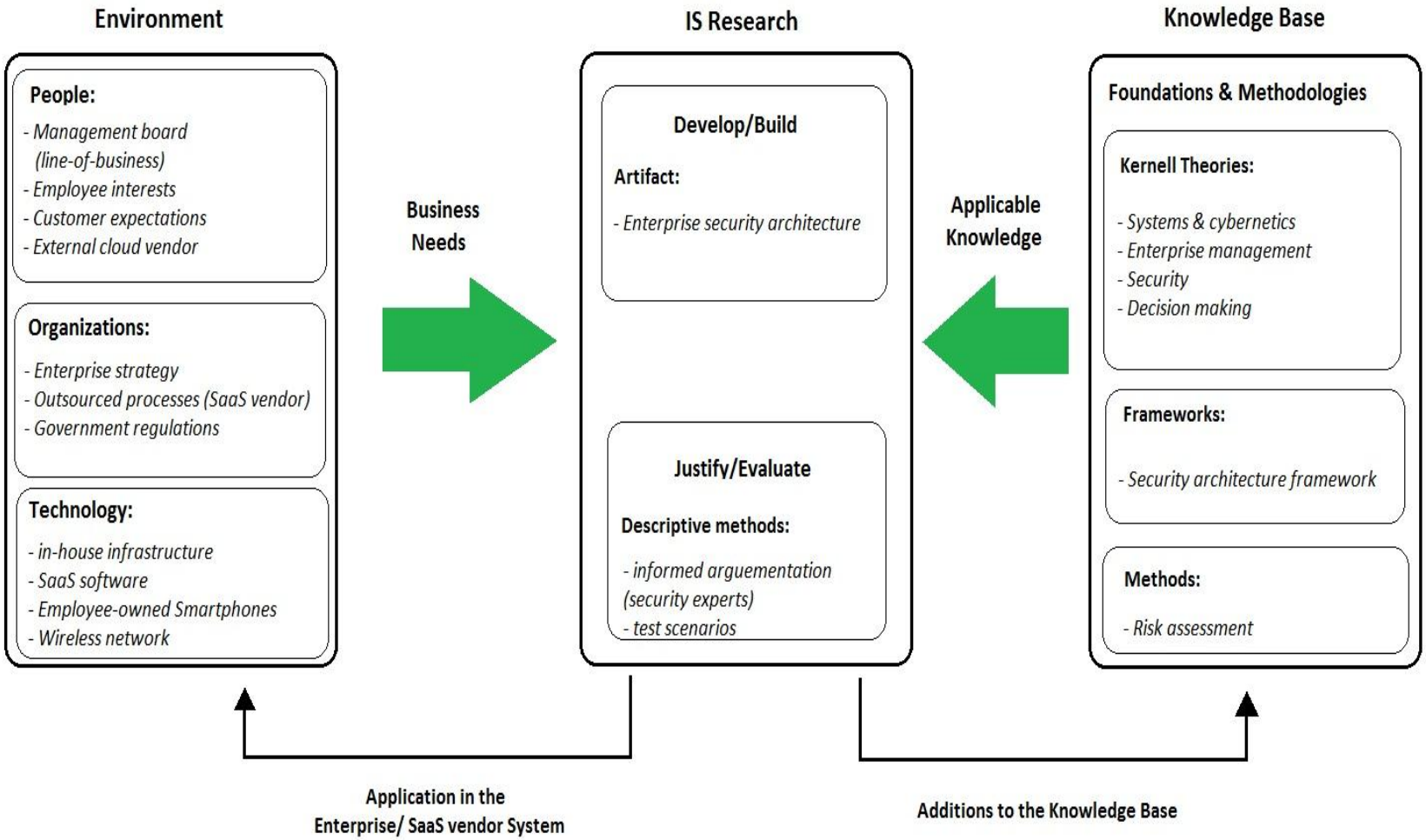

Figure 1 – Information Systems Research framework. Adapted from (9)

1.4.2 Design environment

This Thesis is based on a fictitious case that comprehends an enterprise, which consumes cloud services for carrying out a part of its business processes. Its employees use their personal smart devices in the company and outside to connect to the intranet and directly to the outsourced cloud services. Consequently, the stakeholders' network consists of the management board and the employees of the company, along with the various cloud vendors that deliver the SaaS services and provide the storage space on the enterprise cloud. In addition, European governments play a significant role, as they define the regulations related to personal data access and processing, which might be conflicting with the firms' interests. The relevant technologies utilized by such a fictitious enterprise consists of the SaaS and internal business applications, the on-premises and the cloud vendors' IT infrastructure, the employee-owned smart phones as well as the communication channels through which companies can connect with the employee devices or mitigate their businesses on the cloud.

1.4.3 Research and kernel theories

According to the IS Research framework proposed by Hevner et al. (12), the main goal of this research is to design an enterprise security architecture as the delivered artifact. The IS research involves the iterative processes of building and evaluating the effectiveness of the artifact so that possible flaws or gaps are refined. Kernel theories are applied both on defining the design artifact and during the design process. These kernel theories derive from natural sciences, social sciences and mathematics and govern both the design requirements and the design process of the artifact itself, from the conception up to the implementation phase. The value of kernel theories is to stimulate research on the structural features of information systems' classes in order to offer grounded warrants for the proposed artifact (15).

The relevant kernel theories for enterprise security architectures are mainly systems theory and cybernetics, general enterprise management theories, decision-making theories and security theories (16). Systems theory introduces the concept of a system and the operational processes that are applied within a firm, whereas management theories relate to concepts like strategy, management and control of these processes. Decision-making looks into the different decision strategies and their effects on a specific context. Finally, security theories provide a detailed specification of the allowed and prohibited relationships between subjects and objects according to the stakeholders' security clearance and the security classification of different data types. The design principles that are applied in order to achieve the desired system security logically derive from the aforementioned kernel theories (15).

1.4.4 Frameworks and methods

There are various security architecture frameworks, such as the Service-Oriented Modeling Framework (SOMF), the Extended Enterprise Architecture Framework (E2AF) and the Sherwood Applied Business Security Architecture (SABSA), which aim to simplify the conceptual abstraction of enterprise information security architectures by structuring the design on specific layers, domains or views (65). This report proposes a security architecture based on the SABSA open framework. SABSA is a risk-based methodology for delivering security infrastructure solutions that support the firm's business initiatives to embrace new technological trends and opportunities. This framework is selected, as it is highly customizable to the business model of each enterprise (64). Table 1 below presents our tailored application of the SABSA model, which starts with the business view, where we define the enterprise business processes. The next layer is the logical architecture from the designer's view, where we describe the logical design requirements that the proposed security architecture should fulfill. This layer is followed by the physical architecture from the builder's view, where we describe a set of security mechanisms that meet our design requirements. The target bottom layer is where the component security architecture is assembled, after selecting and precisely deploying hardware, software and service-oriented components in the enterprise network. The security service management architecture layer relates to the ongoing maintenance of the architectural design and its embedded security components. Due to assuming a fictitious enterprise-cloud environment rather than considering a real-life case, we excluded the time column that is not applicable, whereas the people and location columns are only answered in a high-level abstraction.

In addition, the knowledge base includes a risk assessment methodology that is used to identify the information risks for enterprises adopting Smartphone BYOD policies and SaaS clouds, based on which the appropriate security components will be selected to reduce the overall risk to an acceptable level. The risk assessment method is selected upon comparing a set of available methodologies and is analyzed in detail later in this report.

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks

Table 1 - The SABSA matrix. Adapted from (64)

1.4.5 Design research guidelines

The research follows Hevner et al. Design Research Guidelines as described below (12).

Guideline 1 Design as an Artifact: The artifact of this design-science research is a component security architecture for enterprises that adopt SaaS cloud services and Smartphone BYOD policies, based on the SABSA framework. The proposed architecture aims to reduce the relative information security issues to an acceptable level.

Guideline 2 Problem Relevance: The proposed component security architecture can be linked to the enterprises' business goal of providing their services in an efficient, green and profitable way. The importance of the research is justified due to the accelerating pace of cloud computing and Smartphone BYOD adoption by firms in all business sectors.

Guideline 3 Design Evaluation: The overall evaluation of the designed security architecture is based on descriptive methods, mainly via informed argumentation with the help of security experts, as well as through a construction of scenarios that assists in demonstrating the artifact's utility.

Guideline 4 Research Contributions: The design-research contributes in the knowledge base for security measures in enterprises, a secure collaboration with cloud service vendors and the efficient adoption of consumerization (Smartphone BYOD) trends.

Guideline 5 Research Rigor: The rigorous methods that are applied in the construction and evaluation of the component security architecture consist of Hevner et al. IS Systems Framework and Design-Science Research guidelines as described in this section of the Master Thesis report.

Guideline 6 Design as a Search Process: The search process in order to design the desired component security architecture is based on systematic literature review that is conducted on the information technologies and processes that take place in a system comprising the enterprise and an external SaaS cloud. By assessing the aforementioned information and through critical thinking, the main risks that derive from the combination of Smartphone BYOD adoption with SaaS clouds are elaborated. Finally the search for security components assists in building up the proposed security architecture.

Guideline 7 Communication of Research: The research results are communicated to both technology-oriented and management-oriented audiences. Each party examines the viability of the security architecture from its own perspective before a real-case application can take place.

1.5 Structure of Thesis

Upon describing the main concepts in the research domain as well as defining the research objective and the appropriate methodology to accomplish it, we provide in this section the outline of the Master Thesis report, which describes the sequence of the activities that are conducted. The structure of the overview is based on the Design Science strategy, as described in the section 1.4.

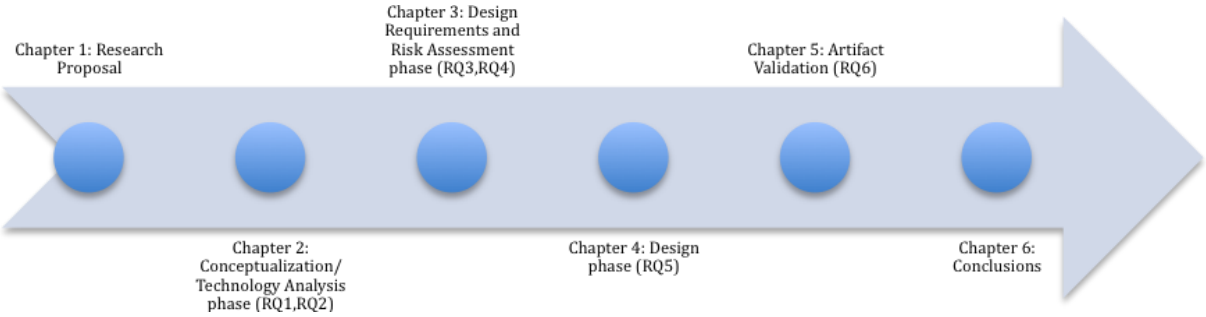

Figure 2 - Thesis outline

As illustrated in Figure 2, the deliverables of the Master Thesis report are the following 6 chapters. Chapter 1 provides an introduction of the Thesis, describing the research problem, research objective and the research strategy that leads to the research goal. Chapter 2 describes the conceptualization and technology analysis phase, where the processes that take place within the system at stake, as well as the underlying IT infrastructure that the aforementioned processes depend on are elaborated in detail through a thorough literature review. Chapter 3 comprises the design requirements and risk assessment phase, in which we examine the basic security and legal requirements and we identify the risks raised for enterprises when accessing SaaS cloud services by Smartphone BYOD. Next, in chapter 4 the utilization of a guideline on security controls takes place, in order to deploy appropriate security components that resolve the issue at stake. The proposed design is based on the knowledge base, as this is established in the previous chapters. Finally, in Chapter 5 the effectiveness of the security architecture is checked for its validity. The validation of the proposed design is conducted via communication with security experts, who assess the architecture on predefined criteria. The conclusions and reflections on the Master Thesis report, with regard to the findings on the research questions and the research objective, as well as the implications for further research that needs to be conducted are described in chapter 6.

Chapter 2: The Domain around Smartphone BYOD

2.1 Theory on business processes

Business processes constitute the centerpiece for enterprises, around which companies can structure their operations, evaluate their performance and gain their competitive advantage. In more detail, business processes are defined as a collection of structured activities or tasks that can create value by turning inputs into valuable output. Each business process is designed for a particular customer that requests a specific product or service. The business process is triggered by the business event related to the aforementioned request and delivers the outcome to the process customer. Business processes can be broken down into sub-tasks that are performed by humans or machines that make use of the company's supplies, such as workstations and raw materials. Consequently, business processes fall under the general management processes, through which enterprises can align their IT infrastructures with the corporate business scope (32).

Common enterprise business processes include applications that companies use to perform functions related to e-commerce, supply chain management (SCM), customer management (CRM), human resources management (HRM) and collaboration services, such as email, document and image management. In contemporary times, companies need a specialized and customized IT support when delivering such services, in order to maintain their business agility (26), (33).

2.2 Enterprise perspective on cloud computing

The emergence of cloud computing as a prominent agility-enhancing technology nowadays has led enterprises to change their focus from deploying and supporting business applications in-house to managing the services that SaaS applications provide, in order to gain a competitive advantage in the market. Companies are realizing that by tapping into the cloud they can benefit from a faster access to better business applications, while boosting their infrastructure resources (1). Compared to the conventional in-house solution, the SaaS model offers some unique features. SaaS applications can be deployed much faster and with minimal effort, which is a crucial factor for enterprises (26). What is more, SaaS applications take advantage of the benefits of centralization through a single-instance, multi-tenant architecture, through which they provide a feature-rich experience competitive with comparable on-premise applications (26). Amongst others, SaaS services offer scalability, rapid provisioning and elasticity, which allow firms to adapt their business according to changes in consumer needs and preferences. At the same time, SaaS solutions provide better protection against network attacks via real time detection of system tampering and other on-demand security controls (1).

In contrast to on-premise services, SaaS application access is sold based on a subscription model, with enterprises paying an ongoing fee to use the application. The fees vary from a flat rate for unlimited access to some or all of the application's features to varying rates according to usage of the service. As a result, SaaS solutions eliminate or drastically reduce the upfront commitment of resources, since the on-demand, multi-tenant delivery model does not require the deployment of a large infrastructure within the enterprise (26). In addition, SaaS services reduce the costs related to disaster recovery (1). Since SaaS services lower the firms' Total Cost of Ownership and improve their Return On Investment, the delivery of business services over the cloud has nowadays achieved a prosperous development. Examples of widely adopted SaaS services include Saleforce's Customer Relationship Management (CRM) and Employease's Human Resource Management (HRM) service (31).

From a technical perspective, the SaaS applications are hosted centrally on the cloud provider's network. This allows SaaS providers to deploy upgrades to applications transparently. From the end-user side, SaaS applications are accessed through Internet by web browsers. Consequently the endpoints accessing the service vary from in-house corporate computers to portable devices, such as mobile phones, netbooks and smart tablets (26).

With more and more line-of-business applications getting delivered through the SaaS delivery model, enterprises are presented not only with greater number of vendor options, but also increased choices for where and how the applications are being delivered. Thus, enterprises are able to trade direct control for the additional flexibility in order to optimize the strategy and execution of their core mission (29).

A typical enterprise case of business process outsourcing to external SaaS providers is shown in the following figure.

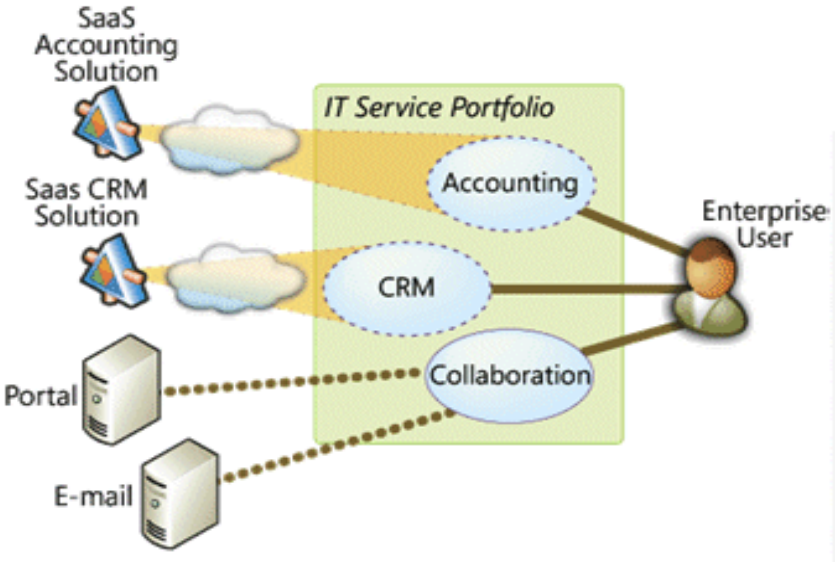

Figure 3 – Enterprise service portfolio

2.3 IT Consumerization in the enterprise

2.3.1 Defining Smartphone BYOD policies

The concept of consumerization of IT relates to the introduction of new information technologies that are firstly adopted by individuals and then spread into business and government organizations. Nowadays, consumerization revolves both around the usage of new hardware, such as Smartphone devices and the utilization of widespread services, such as social media and cloud services. Consequently, the Smartphone BYOD paradigm that derives from the general consumerization trend refers to mobile employees bringing their own smart phones into their workspace, which they use for both business and personal purposes. Smartphone BYOD is becoming more desirable for IT managers, since it assists new trends in the workplace such as remote work, cloud computing and work-shifting. What is more, enterprises benefit from the cost reduction on operational costs, since mobile employees can use their personal smart phones instead of requiring additional hardware purchases within the company. The Smartphone BYOD phenomenon boosts work productivity, as mobile employees are offered with more opportunities to collaborate when using their preferred devices (34).

2.3.2 Security concerns on Smartphone BYOD

The consumerization trend has created new security challenges for IT departments. The technology diversity that Smartphone BYOD policies introduce within the enterprise is now shifting the focus of management from platforms to applications. Due to the threat of confidential corporate data leakage through the employee smart phones, corporations need to ensure that the Smartphone devices are adequately managed so that security is not compromised (34) (40).

In spite of the current security mechanisms that enterprises implement, the evolution of BYOD to Bring-Your-Own-Software (BYOS), related to the installation of personal SaaS applications on the employees' smart phones, threatens to sweep past all corporate defenses and carry away the company data (2). So far, enterprises dealt with this issue through a lock-in under a single umbrella, which can be either a private cloud or a single public cloud provider, while blocking all external cloud applications (28). However, even when organizations block these applications from being executed on-premise, there is the chance that their employees will still use them when they're not connected to the corporate network (2). What is more, a tight control of the personal devices can lead to reduced satisfaction from the end users' point of view, due to the frustration of employees when being forbidden to use additional applications of their preference (34), (36). At the same time, the application of strict control rules affects the performance of the enterprise network, as it practically eliminates the flexibility that Smartphone BYOD polices offer and consequently slows down business (36).

As employees tend to create an "anywhere, anytime" data availability requirement, by collaborating more with suppliers, partners and with each other, regardless of their physical locations, this is driving the proliferation of cloud-based applications, causing a

security and control issue for IT departments, defined as cloud sprawl. Current mechanisms in enterprise security architectures lack the ability to secure the Smartphone users' access and sharing of files through public cloud providers of their choice (2). Consequently, the reliability and security of contemporary security systems is still insufficient for a seamless integration of Smartphone BYOD policies and SaaS services in the enterprise business processes (37).

2.3.3 Defining cloud sprawl

Cloud sprawl is defined as the uncontrolled use of public cloud services in an enterprise with little or no input from management or IT, which can lead to redundant services and increased security risks (2). Cloud sprawl creates a critical security gap for the organization's processes, which derives from the enterprise's lack of control on the security measures that can be implemented on the employee-owned smart phones (18).

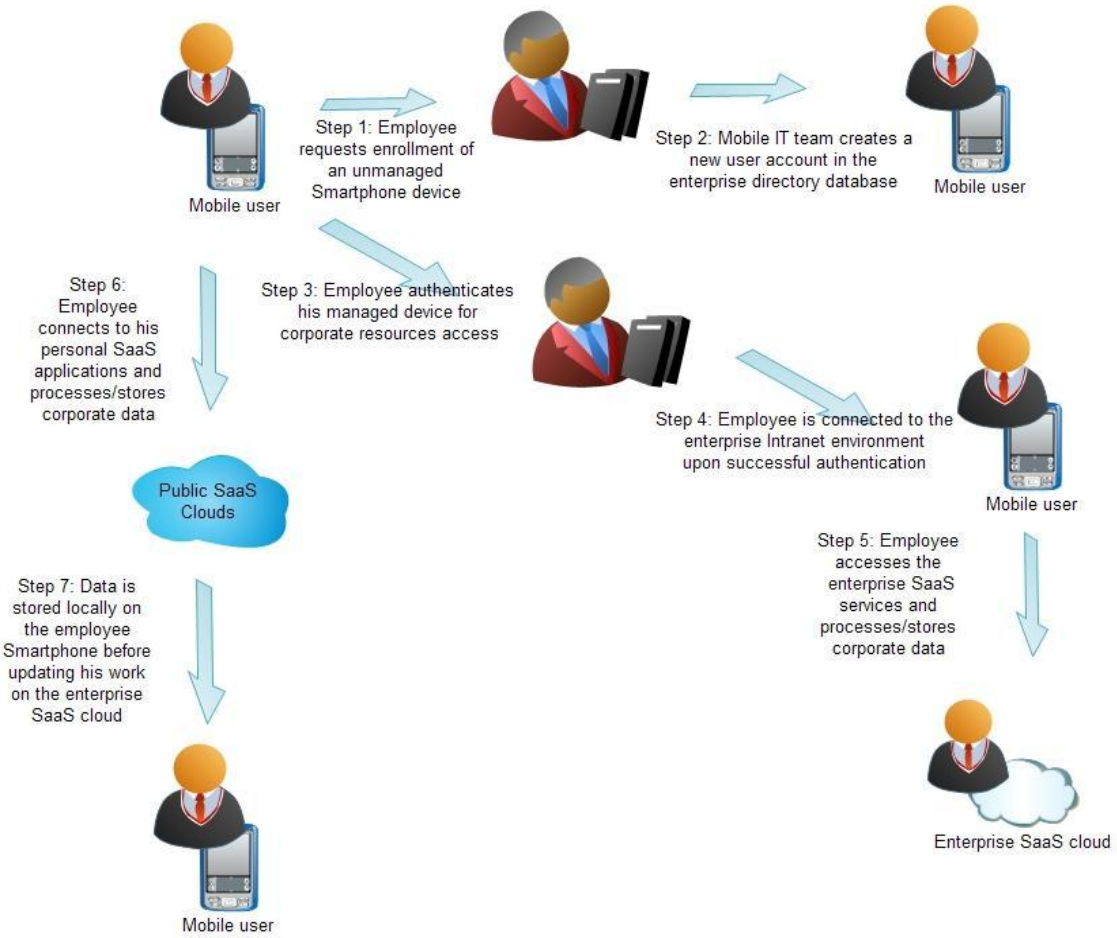

Figure 4 – Cloud sprawl scenario

As illustrated in Figure 4 above, the issue of cloud sprawl can be addressed through a common scenario that occurs when the enterprise adopts a specific cloud storage solution, such as SkyDrive, whereas employees may choose DropBox or Apple iCloud for processing/storing corporate data. In this case of BYOS the corporate data need to be stored locally on the employee device and then has to be uploaded on the enterprise cloud environment. Consequently, a risk of sensitive data being disclosed may occur both at the Smartphone device and the public cloud environment.

The access of personal cloud accounts through the employee smart phones is not compliant with the company's regulations and the inability of the IT management board to audit usage of such public clouds can set the corporate data at risk. The main issue that cloud sprawl raises is related to corporate data remanence on public clouds and on employee-owned smart phones, which don't meet the enterprise security requirements. In this sense, there is the chance that mobile employees forget to delete confidential data from their personal accounts and devices. Even upon request of deletion of the files from a public cloud, cloud storage providers might maintain backup copies to ensure reliability, while end-users are not aware of their existence, which can lead to enterprise data leakage (27). Moreover, the lack of control on the employee-owned smart phones raises concern for IT managers about the software that an employee installs on his device, which might contain malware that can access and replicate confidential data without the owner's awareness (40).

2.4 Stakeholder overview

A vast number of corporate and external stakeholders with conflicting views and interests are related to the adoption of Smartphone BYOD policies in the enterprise. A distinction between the different groups of actors can be defined based on their role of enabling or hindering the implementation of mobility policies in the enterprise. This diversity in Smartphone BYOD approaches is explained by describing different key actors' point-of-views on mobility policies in the following section. An overview of all stakeholders involved along with their roles and interests is presented in Table 2.

External stakeholders, such as Smartphone vendors and ISP/cellular data providers enable the utilization of smart phones for work purposes, by providing the necessary hardware and communication channels (36), (45). In the same sense, cloud partners exert stronger influence on the enterprise's mobility policies by delivering the SaaS business applications, while maintaining security responsibilities on the enterprise cloud (1), (19). However, the variety in available hardware, communication channels and SaaS software can hinder the adoption of Smartphone BYOD, due to the added complexity in the enterprise-cloud environment (36).

On-premise stakeholders also have conflicting views on Smartphone BYOD. On the one hand, IT managers are interested in adopting Smartphone BYOD policies to reap the scalability and flexibility benefits, and therefore need to ensure that sufficient security measures have been implemented before employees can use their personal smart

phones to process corporate data (40). On the other hand, employees can hinder the adoption of Smartphone BYOD, due to their preference for using smart phones for personal needs as well (accessing email accounts, social media etc), which can lead to leakage of corporate data (2). Mobile employees influence the enterprise's mobility policies with their data privacy rights, which the enterprise should not violate during the monitoring of personal devices (47).

Stakeholders	Role	Influence	Interests
Enterprise (Line-of-business)	Enable	High	The IT board's goal is to securely integrate cloud computing services and Smartphone BYOD policies through an enhanced security architecture
Firm's employees	Enable/ Hinder	Medium	Can put the corporate data security at risk by utilizing their smart phones for personal interests that conflict with the firm's policies
Customers	-	Low	Require that their personal information is kept private and that the services rented are delivered timely and in a secure way
External cloud partners	Enable/ Hinder	Medium	Create the need for additional policies to establish a secure mitigation of business processes on the cloud
ISP/Cellular data providers	Enable	Low	Provide the communication channels to enable the remote work of employees through their personal smart phones
Smartphone vendors	Enable/ Hinder	Low	Increase the complexity of the security architecture by offering a variety of Smartphone platforms that the enterprise needs to secure.
Governments	Hinder	High	Enforce data privacy regulations that the enterprise should comply with

Table 2 – Key stakeholders involved

2.5 Information flow between the entities

2.5.1 Device access methods

As already described, in a classic cloud sprawl scenario mobile employees may use their smart phones for both personal and business purposes. The different device access methods for the enterprise and cloud environments are illustrated below, in Figure 5.

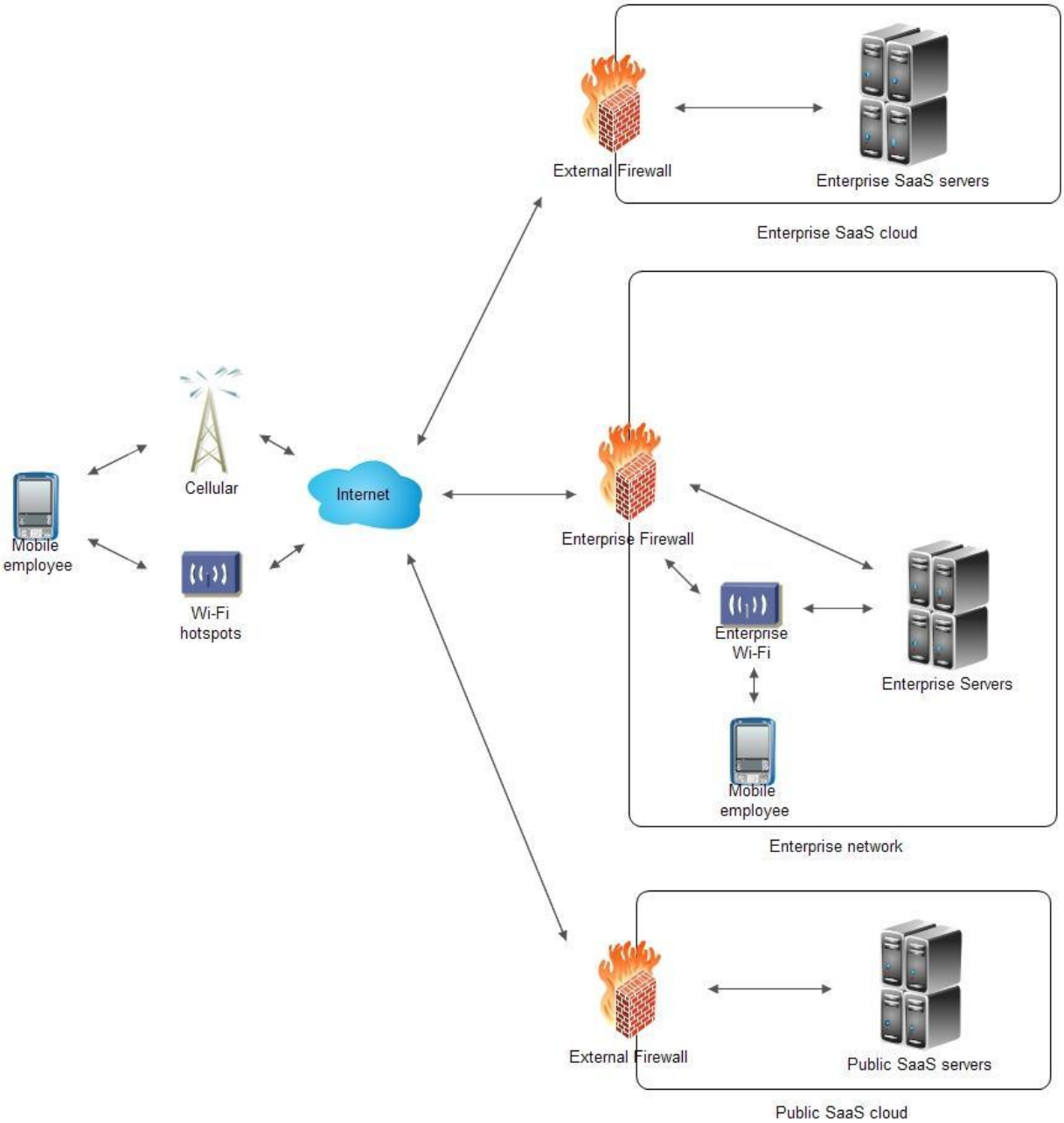

Figure 5 – Device access methods

When using their personal smart phones for accessing the in-house and enterprise cloud business applications, employees may connect to these corporate services both remotely and directly via the enterprise wireless network.

In the case of remote work, access to the in-house Line-of-business (LOB) servers is provided to mobile users upon establishing a connection to the Internet, either via a Wi-Fi hotspot or via the Smartphone's cellular data connection. Whereas the enterprise cloud servers can be directly accessed in the same way, the integration of external SaaS applications in the enterprise service portfolio can provide an alternative access method of the enterprise cloud via the corporate network (29).

On the other hand, when employees work within the enterprise environment, direct access to the in-house and the enterprise cloud services is provided via the enterprise Wi-Fi network. An alternative access route to the enterprise cloud via the enterprise servers is also offered when employees use their smart phones within the company (29).

The aforementioned device access methods also apply to public SaaS cloud access scenarios. In this sense mobile employees can access their personal accounts on the various public cloud environments both remotely, by making use of Wi-Fi hotspots or a cellular data network, and while working on-premises via the enterprise Wi-Fi (8).

In all cases, the incoming and outgoing network traffic for in both the enterprise and the external cloud environments is by default controlled via the deployment of firewalls (58).

In the following section, the information flow between a Smartphone device and the various personal and business applications is described in detail.

2.5.2 Information flow in public SaaS clouds

Public SaaS clouds are accessed by mobile users via a web server upon connection to the Internet, either via a Wi-Fi connection or via the Smartphone's cellular data network. When accessing personal cloud services, mobile employees connect to the cloud environment by using their individual usernames and passwords. By default, the user credentials are processed by an authentication server that compares input with the user database directory that is located on the cloud provider environment (8). If the public cloud involves a set of applications, such as the case of SaaS office suites, the mobile user has single sign-on access to all internal services of the cloud vendor (2). Upon successful authentication the public cloud provider ensures the secure application and storage space access to the authenticated user. Nevertheless, the accessing of personal cloud accounts via employee smart phones entails the risk of mobile employees transacting business in a way that cannot be monitored by the company (44).

2.5.3 Description of the enterprise network

By default IT managers deploy in the corporate environment a Smartphone management server, which enables the communication between the enterprise and the mobile devices (37).

Before an employee device can be used to process business data, it has to be enrolled in the enterprise environment as a new account in the company's active directory database (35), (41). In this way, only the managed devices that establish authenticated connection to the enterprise network can access the corporate applications and data (40). Registered Smartphone devices that request access to the enterprise network can authenticate through the Smartphone management server (37). In this aspect, such a server becomes the access gateway to the company's IT resources (30).

At the same time, the Smartphone management server allows mobile IT managers to send instructions back on the authenticated Smartphone devices, in order to control the user access to the enterprise IT environment, depending on the nature of the accessing users, the location of their access and the type of Smartphone that is used (36), (37).

Consequently, there should be constant bilateral communication between the mobile devices and the corporate Smartphone management server.

2.5.4 Information flow within the corporate network

When working outside the enterprise premises, mobile employees can connect to the LOB servers via a Wi-Fi or their cellular data connection. For the first option, mobile devices are routed to the internet upon gaining access to third-party owned Wi-Fi hotspots, including their personal internet connection at home, which are usually protected by an IEEE 802.1X password. When using the standard cellular mobile data service (i.e. 3G/4G long-term evolution (LTE), General Packet Radio Service (GPRS) or Code Division Multiple Access (CDMA)), mobile devices make use of the data network of the cellular providers, and then connect to the Internet via the Mobile Operator IP network (45). The default Smartphone management server provides an authentication mechanism that grants access to the business servers by comparing the remote employee input with the enterprise's active directory database (37).

The information flow in the case of remote work is illustrated below, in Figure 6.

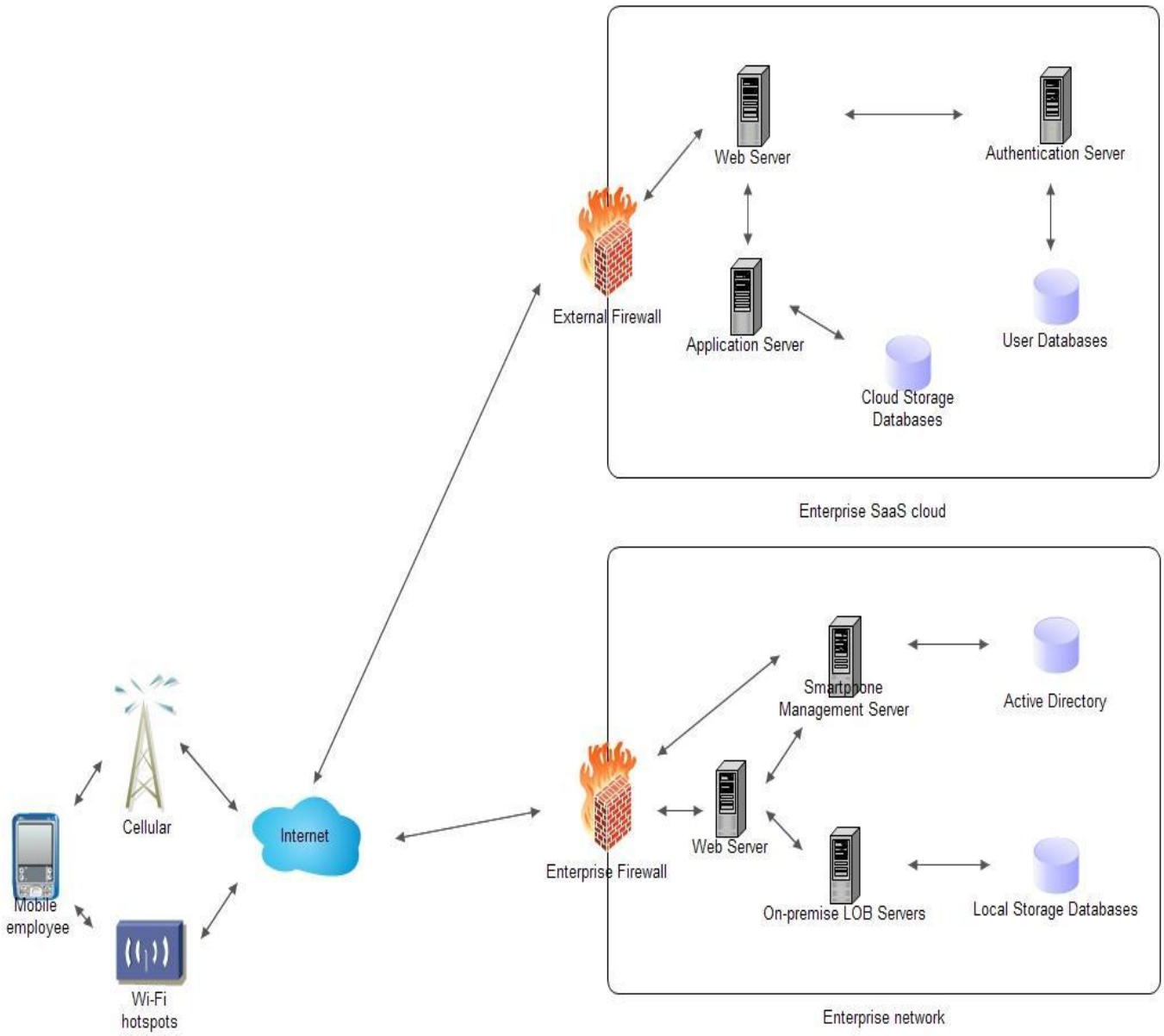

Figure 6 – Remote work information flow

When employees connect locally to the internal enterprise Wi-Fi, a direct access of on-premise applications is undesired and therefore not adopted by companies, as this approach would require the storage and managing of separate credentials in order to authenticate for each business service (39). Alternatively, enterprises can make use of the default Smartphone management server, which can authenticate smart phones centrally by comparing employee credentials in the company's active directory (35).

The information flow when mobile employees connect to the enterprise and personal services via the enterprise Wi-Fi network is illustrated below in Figure 7.

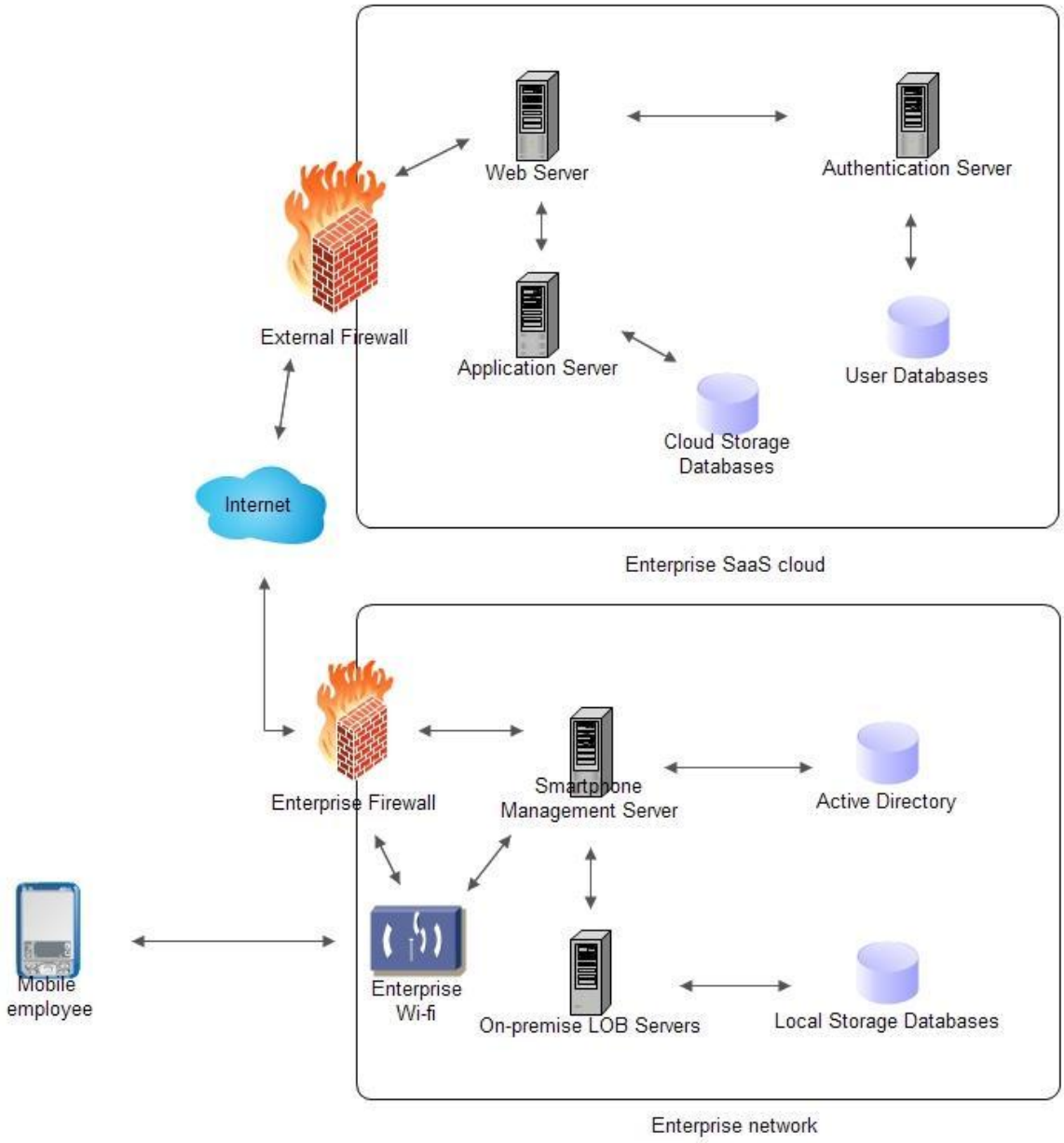

Figure 7 – On-premise work information flow

2.5.5 Accessing the enterprise SaaS clouds

Upon establishing an Internet connection, mobile employees may access the enterprise cloud directly via a standard authentication procedure on the cloud provider's environment. On the other hand, when connecting to the enterprise cloud through the enterprise servers, employees can gain access to the external SaaS applications by authenticating their session within the enterprise via the default Smartphone management server that that interfaces with the company's active directory, where employee accounts are stored (43). An on-premise user authentication provides

consistency and convenience for both employees and IT managers, since there are fewer sets of credentials that need to be checked and less security issues related to the loss or misplacement of passwords (30). At the same time, this identity integration approach could allow managers to implement universal access policies instead of managing permissions individually for each application.

2.6 Current security landscape

Based on the presented context, as it was described in section 2.5, we assume a modest information security architecture to be already present in the enterprise-cloud environment. In this sense, we assume that the fictitious enterprise implements by default a number of basic technical controls, so that employees can securely process corporate data that are located in the enterprise LOB and cloud servers via their personal Smartphone devices. At the same time, such controls prevent attackers from both accessing/modifying the enterprise's confidential information and harming the system's availability through flooding or denial-of-service attacks (59).

More specifically, the corporate data at rest, which is located in the in-house and enterprise cloud servers, is protected via a standard encryption algorithm in order to ensure data integrity and confidentiality (58).

Enterprises prevent unauthorized users from accessing the corporate data via a basic access control mechanism. This mechanism is based on identification and authentication of employee owned Smartphone devices using username and password pairs that are stored in an active directory within the enterprise. A similar authentication mechanism is used for controlling the access of employees to the enterprise cloud; in this case, user credentials are stored in a database located on the cloud vendor environment. Such mechanisms ensure authenticity for the system at stake. The access control mechanisms are configured in a way that prevents low-level employees from accessing specific sensitive in-house and cloud data/services. The authorization to access information and services is defined by the enterprise's administrative policies (58).

When employees access business services within the enterprise via the wireless corporate network, an additional security control in place is the encryption of the Wi-Fi access via password authentication (45).

Within the enterprise network, anti-virus software is installed on the corporate servers and local computers so that malicious software, which can harm data integrity or lead to disclosure of confidential information, is detected and blocked (58).

An additional security control that is used to prohibit access to sensitive business data are firewalls, which are placed at the border of the enterprise network, so that any type of incoming and outgoing network traffic is monitored. Firewalls define which data packets are allowed in or out of the enterprise network, thus preventing unauthorized access and ensuring data confidentiality. In the same way, firewalls are deployed at the

border of the enterprise cloud, as the default security mechanisms for the cloud environment (58).

On top of these measures, enterprises formulate Smartphone policies that provide the guidelines on the services allowed on the Smartphone devices. In a similar way, enterprises formulate policies regarding the relationship with the external cloud partner, in order to protect the corporate data that is stored and processed on the cloud environment. Along with enterprise policies, firms apply organizational security measures, related to the education and training of employees on how to use their smart phones for business purposes without putting the corporate data at risk (59).

Physical controls are also part of the security mechanisms that enterprises apply, in order to protect the corporate assets from intruders and ensure service availability in spite of disruptions due to hardware or power failures. Such controls involve the hiring of security guards and the implementation of locks and perimeter fencing for the enterprise facilities, as well as the installation of uninterruptible power supply (UPS) devices as a backup power solution (59).

An overview of the fictitious though not unrealistic enterprise-cloud system's current security landscape is illustrated in Figure 8, below.

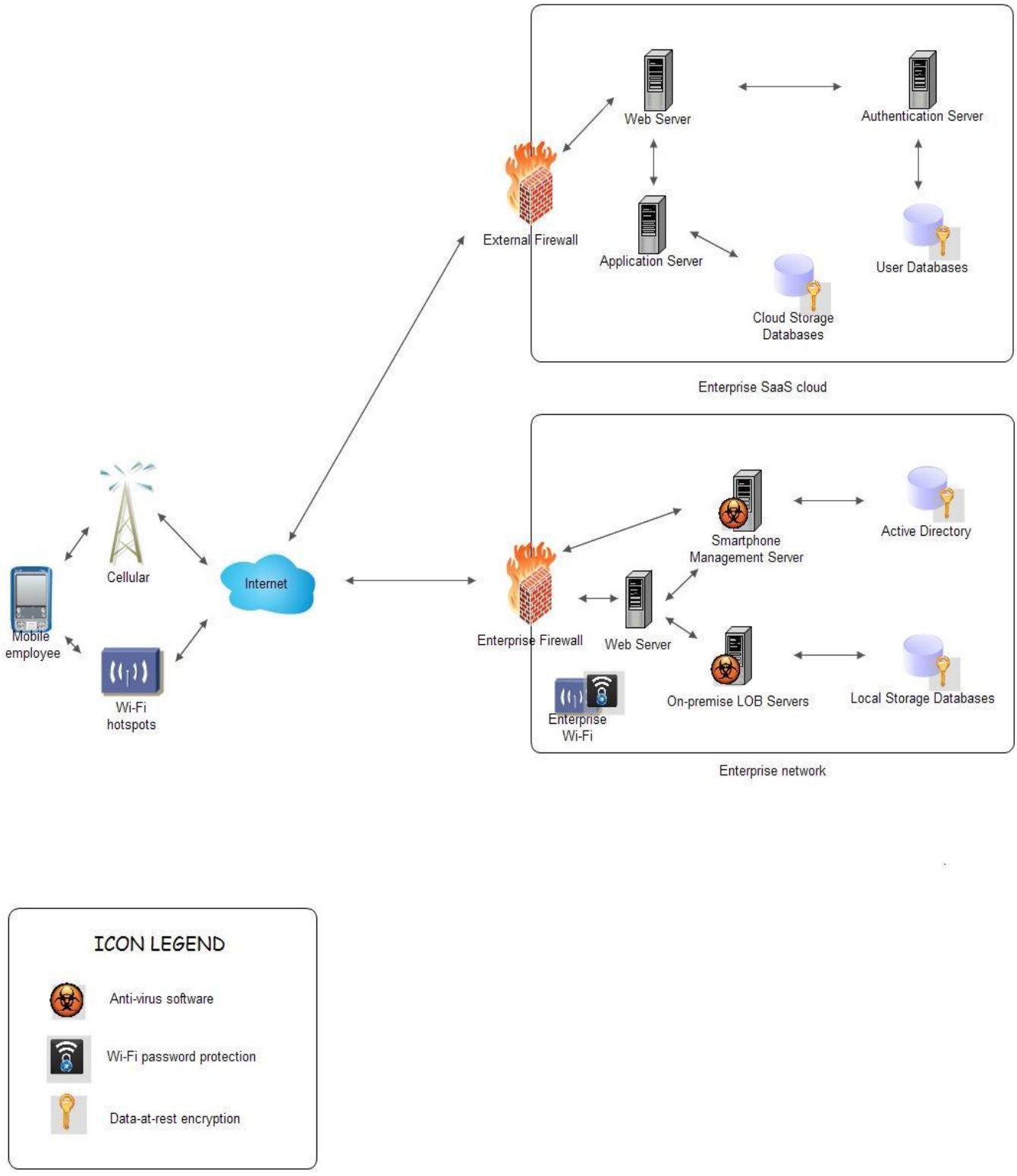

Figure 8 - Current security landscape

2.7 Conclusions

In this chapter the importance of business processes for enterprises has been discussed. After the introduction of SaaS business solutions in the market, enterprises consider the outsourcing of business applications to external cloud providers. Their need for more flexible and cost-efficient operations has also led to the adoption of Smartphone BYOD policies that enable remote working via employee-owned devices. A description of remote working processes and the enterprise's current technical domain was also given in this chapter. In this sense, chapter 2 described the contextual architecture layer of our customized SABSA model. In paragraph 2.3.3, the discussion on cloud sprawl explains why the adoption of mobility and cloud technologies by enterprises is not problem-free. Such concerns can be seen as a risk for the enterprise. Risks of Smartphone BYOD adoption are the central subject in this research and are therefore elaborated later in this report.

This chapter has provided the answer to the first research question, which was:
"What are the relevant business processes that take place amongst the different stakeholders involved in the enterprise-cloud system?". This question is answered by the illustrated interrelations between a Smartphone device, the enterprise internal network and the enterprise cloud, as presented in Figures 5-8.

This chapter has also provided the answer to the second research question, which was: "What is the underlying IT infrastructure in the enterprise-cloud system?" This question is answered by the technical components within the enterprise cloud and internal network that are illustrated in Figures 5-8.

Chapter 3: Design Requirements and Risks around Smartphone BYOD

3.1 Information security requirements

Information security, as defined by the ISO 27001 standard, revolves around the following five core principles: confidentiality, integrity, availability, access control and non-repudiation (66). Confidentiality relates to the protection of information from intentional or accidental disclosure to parties that are not intended to receive it. Data integrity means that data should be accurate and consistent throughout its entire life cycle. In this sense, data should not be modified by unauthorized users or in an undetected manner. Data availability requires that all computing systems that process, store or protect the data, as well as the communication channels between the different system components, are functioning properly. The data itself should be available whenever it is needed. Access control is defined as the prevention of unauthorized use of a resource and is realized via authentication and authorization. Authentication provides the means of verifying that the parties involved in data processing are who they claim to be. Authorization provides a means to specify and manage the allowed actions for each actor involved in a system. Non-repudiation implies that during a transaction both the receiving and the sending party cannot deny having received or sent the data respectively (59), (66).

The above requirements are needed for enterprises that implement Smartphone BYOD policies and cloud computing technologies, due to the multi-tenant nature of the enterprise cloud environment and the exposure level of the employee-owned devices. More specifically, due to the fact that a single cloud hosts all types of data classifications that derive from multiple customers, it is necessary that the corporate data confidentiality and integrity is protected from malicious persons during its transmission, processing and storage on the cloud. Consequently, an access control mechanism is required to ensure that data reads or modifications are carried out only by authorized personnel and according to their job permissions. The enterprise data should be available whenever an authorized remote or local employee requests access, whereas non-repudiable proof on the identity of the person performing any type of activity should be present. The employees' combined use of smart phones for business and personal purposes further explains the need for the above security requirements, since the confidentiality and integrity of business data should be protected from personal applications that might contain malicious codes and the access of corporate data by third-persons that may use the Smartphone devices (i.e. the employees' family members, friends etc) should be controlled.

3.2 Legal requirements

In addition to the aforementioned security requirements, enterprises implementing Smartphone BYOD policies and SaaS applications should meet a number of legal requirements, which mainly relate to applicable laws on the remote monitoring of workers (47). In addition, cloud-computing technologies pose further legal issues that affect the firm's BYOD policies, which should also be addressed before designing an effective security architecture. Since our proposed solution is targeted for European countries, the main EU directives and regulations regarding Smartphone BYOD are identified and elaborated in the following section.

The main constraint for enterprises adopting Smartphone BYOD policies relates to the privacy of both enterprise and employee personal data on the Smartphone devices. Whereas the corporate mobility policies indicate that employees are allowed to make use of their own smart phones for business-related tasks, they involve a set of rules in order to protect the enterprise from the case of destruction or leakage of confidential corporate data. In this sense, mobility policies indicate that personal devices are monitored to ensure that all employee activity and enterprise data access via the personal devices is in line with the corporate rules. This entails the danger of the corporation breaching its employees' data privacy rights, which would lead to reduced work satisfaction and even lawsuits against the enterprise (56).

The legal environment around data privacy in the European Union is created by the "General Data Protection Regulation" (GDPR). In addition, each European country has its own set of regulations concerning enterprises that implement mobility policies. More specifically, data privacy in the Netherlands is governed by the Dutch Data Protection Authority, which supervises the compliance and application of the Dutch "Data Protection Act" (DPA), the "Police Data Act" and the "Municipal Database Act". Further data protection legislations that are examined in this research are the German "Federal Data Protection Act", the Spanish "Organic Law on Data Protection", the French "Law on Protection of Data Subjects as Regards the Processing of Personal Data" and the UK "Data Protection Act" (DPA) (47), (56).

Despite the fact that each of these countries enforces data privacy laws in a national level, they all include a number of main principles that have an impact on enterprises implementing a Smartphone BYOD policy. These principles are elaborated below.

Although employees use personal devices to perform business tasks, enterprises still play the role of the data controller (54). In the case of sensitive corporate or personal data being lost, leaked or misused, the enterprise is held responsible and therefore runs the risk of being fined by the local data regulatory authority. Consequently, companies should implement security controls in order to protect sensitive data that are accessed and processed through the employee smart phones, including both employee and client/business information (47). In more detail, this entails the protection of data stored and transmitted to and from the smart phones by applying a number of technical

controls on the devices and the communication channels with the company network. Additional/alternative controls should prevent specific types of data from being stored locally on personally owned devices (56). What is more, organizational controls should be in place to ensure employee compliance with the enterprise's data privacy regulations/guidelines. A formal reporting mechanism for all data loss incidents is another organizational measure that should also be implemented (47).

From the employee perspective, an enterprise's attempt to secure data by accessing and controlling the employee-owned smart phones can be approached as an invasion of individual privacy rights. As a result, all relative legislation across Europe dictates that employees must give fully informed and unambiguous consent before the organization can access and process their personal data. Enterprises are legally obliged to inform employees about the exact activities that will be monitored and the kind of data that will be collected from their personal devices. Further information should be available to employees, relating to the way that personal data will be used and the people that will access it (47), (55).

In any case of employee data being collected, the enterprise actions should be compliant with the purpose limitation principle. This means that any processing of personal data on employee-owned devices should be for lawful grounds relating to the protection of corporate data and the monitoring of employee abidance by the company policies. All monitoring actions should also comply with the "data minimization" principle, meaning that the collection of personal information should be limited to directly relevant and necessary data to accomplish the aforementioned lawful purposes. Personal data should only be retained for as long as is necessary to fulfill these purposes (54).

In order to provide transparency about personal data collection to their employees, enterprises need to keep an updated record of all breaches of personal data (54). European data protection regulations require that a data protection officer is appointed as the responsible person for any data monitoring and security issues (47).

Additional legal requirements relate to the organization's need for cooperation and agreement with local work councils before formulating its mobility policy (47). What is more, regulations related to the storage of sensitive data on both the Smartphone devices and on the cloud partner's environment restrict the transfer of data outside the European Economic Area, unless an adequate level of protection for the rights of data subjects exists in that location (56).

Table 3 provides an overview of the design requirements that the proposed security architecture should fulfill. This set of requirements constitutes the logical architecture layer of our customized SABSA model.

Category	Design Requirements
1. Organizational – Legal	a. Establish employee consent on personal device monitoring
	b. Provide a detailed record of all personal data breaches during the monitoring of Smartphone devices
	c. Define a set of allowed features on and services accessed by employee-owned smart phones
	d. Ensure that employee-owned devices support a minimum level of security features before allowing to be used for business tasks
	e. Define the cloud provider's access level on the corporate data stored in the enterprise cloud
	f. Define the permitted geographic locations for external storage of corporate data by the cloud vendor
2. Information Security	a. Protect the enterprise business data's confidentiality, integrity and availability, both in transit and at rest.
	b. Protect the Smartphone locally-stored corporate information's confidentiality, integrity and availability
	c. Protect the availability of the enterprise servers
	d. Protect the availability of the Smartphone platform
	e. Provide access control to the internal and enterprise cloud databases and applications
	f. Provide non-repudiation for all corporate data and application access

Table 3 – Security architecture design requirements

The design requirements alone do not suffice in defining the appropriate security controls and their precise positioning on the enterprise-cloud system, which could secure Smartphone BYOD adoption, since the loss of security attributes depends on the different risks that the system at stake entails. Consequently, in the following section a risk assessment methodology is performed, in order to trace the potential gaps in the current information security architecture and as such to place the right controls at the right places to meet the design requirements.

3.3 Information system risk assessment

3.3.1 Theory on risk assessment

Risk assessment is the cornerstone of any information security program, since it enables enterprises to identify their vulnerabilities and weaknesses before IT managers can

proceed with the implementation of adequate security controls. A vast number of IT risk management frameworks have lately emerged. These frameworks aim to assist companies in risk identification, risk prioritization, risk management as well as in defining the tools that build the defense mechanism of the enterprise (51).

A great benefit that risk assessment frameworks offer is that they enable a thorough evaluation of IT resources, so that an enterprise can invest in security defenses more uniformly. This is particularly important due to the "weakest link" nature of security where a single weak component can compromise the entire security process. Consequently, the appropriate allocation of defensive resources is deemed necessary (48).

The following section provides an overview of different methodologies, in order to identify the most suitable risk assessment framework for the system at stake.

3.3.2 Methodology evaluation

ISO 27005

ISO 27005 is an Information Security Risk Management guideline. The guideline is customizable to each company's nature and therefore applicable to organizations of all types and sizes. ISO 27005 advocates an iterative approach to risk assessment through a Plan-Do-Check-Act cycle. The steps involved in the cycle relate to risk analysis and evaluation. In more detail, risks are analyzed by first identifying the assets at stake, the threats that affect each element, the current security controls that are applied as well as the consequences of a threat occurrence. As a next step the measure of each risk is specified through a risk estimation, either quantitative or qualitative. This enables the evaluation of risks by comparing and prioritizing risks based on specific evaluation and acceptance criteria (49).

However, a major drawback of the ISO 27005 is that it provides a general guideline for risk assessment without recommending specific risk assessment methodologies (53).

OCTAVE

In contrast to technology-focused frameworks, the OCTAVE risk assessment method is more targeted at organizational risk and practice-related issues. The OCTAVE framework can be adapted for most types of organizations, as it is a flexible evaluation approach, which is based on two key aspects: operational risk and security practices. In this aspect, OCTAVE examines technology only in relation to the organization's security practices. When applying the OCTAVE approach, the security decisions derive from examining the risks to the confidentiality, integrity and availability of the critical IT assets, through which a firm can formulate a practice-based protection strategy. The OCTAVE methodology starts with the formulation of asset-based threat profiles, in order to determine the most important assets to the enterprise and to describe the current

security controls that are applied on these assets. Upon identifying the vulnerabilities of the current infrastructure, the OCTAVE framework is used to develop a security strategy for the firm as the final step (50).

A drawback of the OCTAVE framework is that it does not make use of probabilities or provide a structured means to determine when a risk likelihood/impact can be classified "high" or "low"; rather it only states that the rating criteria should be meaningful to the enterprise (52). What is more, due to the fact that the OCTAVE framework was developed for large organizations, a multi-layer hierarchy and a large in-house computing infrastructure assumption might not fit the case of small-medium enterprises, when applying the method in such cases (50).

Microsoft Security Risk Management Guide

The Microsoft Security Risk Management Guide comprises four primary stages: Assessing Risk, Conducting Decision Support, Implementing Controls, and Measuring Program Effectiveness. The process assists enterprises in developing a cost-effective control environment by organizing the firm's resources so that to manage and minimize risks to an acceptable level. The Assessing Risk is the first stage of the Microsoft Security Risk Management Guide, during which risks across the organization are identified and it is broken down into three phases related to the planning, data gathering and analysis of risk related information. The output of the risk assessment stage is a prioritized list of risks, which includes both a qualitative ranking and quantitative estimates. The selection and implementation of appropriate security controls during the next stage of the Security Risk Management is based on the risk assessment output (51).

The Security Risk Management Guide involves a number of supportive tools for each phase, through which the risk ratings are calculated. More specifically, during the first phase information risk analysts can use the Project Schedule tool as an assistant for planning the relative activities of the risk assessment stage. In the same sense, the Data Gathering tool can be used during the second phase as a template to assist in facilitating discussions to gather risk data. Finally, the Summary and Detail Level Risk Analysis Worksheets can be used during the last phase as a tool that assists in conducting an exhaustive analysis and prioritization of the key information risks that have been identified (51).

3.3.3 Application of the Microsoft Security Risk Management Guide

Having assessed the three aforementioned frameworks, the risk assessment for the system at stake is carried out based on the Microsoft Risk Management Guide, due its higher depth of analysis as well as due to the limitations related to other methodologies, as described above. A high-level description of the selected methodology is illustrated in the following figure.

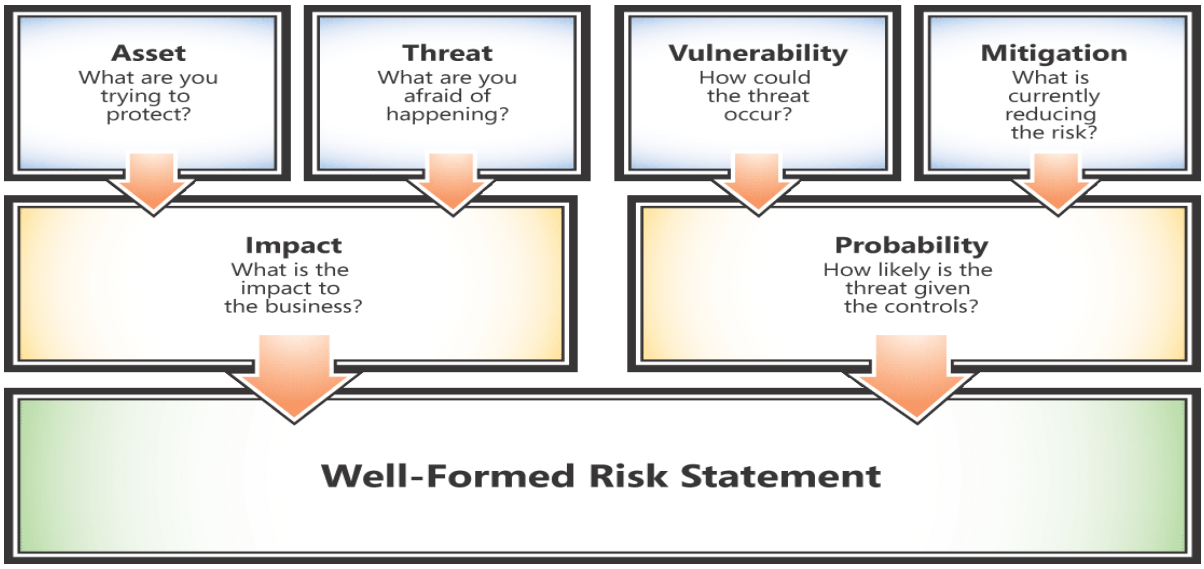

Figure 9 – Assessing Risk stage. Source: (51)

As illustrated in Figure 9, the Assessing Risk stage can be broken down into three phases. The first phase is the planning phase, which builds the foundation for a successful risk assessment by adequately aligning, scoping, and gaining acceptance of the Assessing Risk stage of the Security Risk Management Guide. The next phase is the facilitated data gathering phase, during which risk related information is gathered from stakeholders across the organization. More specifically, the data elements that are collected during this phase relate to the organizational assets, threats and vulnerabilities for the system at stake as well as to current and proposed security controls. The final phase is the risk prioritization phase, where the identified risks are qualified and quantified in a consistent and repeatable process. In more detail, a full list of security risks is derived from a qualitative approach, whereas the most significant ones are subjected to a detailed analysis using quantitative techniques. The risk prioritization phase is subjective in nature since the process relates to predicting the future (51).

Before conducting the risk assessment stage, the key enterprise assets that need to be protected should be defined, due to the fact that the inclusion of all tangible and intangible assets in the risk assessment phase is practically impossible. The asset subset selection is carried out based on FIPS 199, which is a mandatory security categorization standard, whereas the rest of the enterprise assets are expected to be treated accordingly (63). The standard's concept is to determine appropriate security priorities for organizational information systems. These priorities are based on the adverse impact on organizational operations, organizational assets, individuals, other organizations, and the Nation in the case of loss of confidentiality, integrity, or availability. It should be noted here that according to the FIPS 199 standard, information integrity includes ensuring its non-repudiation and authenticity. In this sense, the generalized format for expressing the security category (SC) of an information system is:

SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

The acceptable values for potential impact are low, moderate, or high. The definition of potential impact for each security objective is summarized in Table 4 below.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 4 – Potential impact on security requirements. Source: (63)

An enterprise asset is classified as low-impact when the impact in case of loss each design objective is low for all of them. In the same sense, a moderate-impact asset has at least one moderate impact on the design objectives and no impact on the design objectives is greater than moderate. Finally, a high-impact asset has at least one high impact in the design objectives.

Along with the security requirements, we defined in Table 3 a number of legal requirements that the security architecture should fulfill. However, a potential non-compliance to each legal requirement can be translated as a violation of the relative assets' security requirements. In this sense, a lack of employee consent for their personal data being accessed by the enterprise (legal requirement 1.a) or the lack of transparency in the monitoring process (legal requirement 1.b) would have an adverse

impact in the employee personal data's confidentiality, integrity and availability. The lack of device compatibility with security controls and the lack of predefined permissions on the features and services that are allowed on the employee-owned smart phones (legal requirement 1.c, 1.d) can affect the confidentiality, integrity and availability of both the locally stored business data and the of the data that is stored on the internal and enterprise cloud databases. Finally, the cloud vendors' non-compliance to the cloud servers' location restrictions and their non-compliance to the access restrictions in the enterprise cloud databases (legal requirements 1.e, 1.f) affect the enterprise cloud databases' confidentiality, integrity and availability. Consequently, when classifying the key enterprise assets according to the impact in case of loss of each security requirement the non-compliance to the legal requirements is also implied.

The asset subset that is examined during our risk assessment involves assets from all classes. As far as the high business impact (HBI) class is concerned, all corporate data residing on the in-house and enterprise cloud databases are the most crucial assets for the corporation. These databases contain not only highly important business-related information (such as client details, inventories and business plans) but also the employee credentials for accessing the in-house and cloud business applications. As a result, any loss of confidentiality, integrity (including access control and non-repudiation) or availability related to this asset can be devastating for the enterprise. In the same sense, a potential compromise in the firm's critical infrastructure (i.e. the enterprise servers and data centers) would severely harm the enterprise, both in direct financial losses and a tainted brand image. MBI assets have a moderate impact on the organization. For an enterprise adopting mobility policies and cloud computing technologies, MBI assets relate to the power and telephone lines on the enterprise premises, as well as the corporate data residing on smart phones and in-house workstations. Such locally stored data copies constitute only a slice of the overall enterprise data repositories and therefore their potential loss or unauthorized modification would have a moderate business impact, provided that the corporate data centers remain intact. Finally, examples of LBI assets include the on-premise desktops and laptops and the employee-owned smart phones, which are still considered part of the enterprise infrastructure when used by employees for business purposes. The employees' personal information on the Smartphone devices are also classified as an LBI asset of the enterprise, due to the indirect legal consequences for the firm in the event of their privacy being compromised.

Table 5 below provides a high-level overview of the selected asset subset along with their classification based on the business impact in case of loss of each applicable security requirement. A more detailed asset list can be found in Appendix A. It should be noted that the impact class of each asset is defined according to the fictitious rating lists provided by the Microsoft Security Risk Management Guide and the FIPS 199 standard. As a result real-life differentiations amongst the various business domains are not taken into account (e.g. the impact in case of loss of personal data confidentiality is more severe for a healthcare industry rather than for entertainment service renting businesses). Due to the fact that our security architecture is designed to protect the key

identified assets, the proposed asset table should be tailored according to the business environment of each enterprise before conducting the risk assessment stage, in order to optimize the security level offered by our architecture.

Asset	**Impact in case of loss of**			**Impact class rating**
	Confidentiality	Integrity (incl. access control and non-repudiation)	Availability	
In-house corporate databases	High	High	High	HBI
Corporate databases on the enterprise cloud	High	High	High	HBI
Data centers/servers	-	-	High	HBI
Enterprise workstations	-	-	Low	LBI
Corporate data on enterprise workstations	Medium	Medium	Low	MBI
Employee smart phones	-	-	Low	LBI
Corporate data on employee smart phones	Medium	Medium	Low	MBI
Employee personal data	Low	Low	Low	LBI
Power supplies/telephony lines	-	-	Medium	MBI

Table 5 - Asset classification

In a similar sense, the potential threat and vulnerability lists relating to the key enterprise assets, as offered by the Microsoft Security Risk Management Guide are too extensive and have been therefore tailored to the most significant for the specific enterprise-cloud system, based on a subjective selection process. The threats that are taken into account include not only external malicious persons that aim to harm the enterprise's data and infrastructure, but also former and current employees that may deliberately or unintentionally transmit, delete or modify the corporate data for their personal benefit or due to them lacking appropriate training. On the other hand, the tailored set of vulnerabilities in the enterprise's key assets is defined by considering all aspects of security, including physical weak points (e.g. weak door locks), technological gaps (e.g. outdated anti-virus software or weak encryption mechanisms) and

insufficient organizational policies (e.g. lack of a formal acceptable-use policy for Smartphone devices). The complete adapted threat and vulnerability lists can be found in Appendixes B and C respectively.

Each of the selected key assets is addressed for a relevant combination of threats and vulnerabilities. The overall business impact for each threat-vulnerability combination is calculated by first determining the exposure of the specific asset, which is defined as the extent of potential damage occurring on the asset itself, and then combining the asset's class rating with the asset's exposure. Next the probability of the impact's occurrence is calculated by considering both the level of effectiveness of the current security controls on eliminating the specific threat and the different exploit types that may occur. The overall risk level is based on both the impact rating and its probability. While performing the risk assessment, the impact, exposure, probability and overall risk levels are qualitatively estimated, due to our generalized research approach that does not provide us with quantitative input.

The key identified risks for the systems most valuable assets are listed in Table 6 below.

For instance, we identify the unauthorized access to the internal and enterprise cloud databases through theft of employee credentials off a remote client as a significant threat that affects the corporate databases. This threat is possible to occur due to a lack of security controls on an employee-owned Smartphone that makes it vulnerable to attacks. The unauthorized access to corporate databases completely exposes the asset itself, which consequently has a high overall impact for the enterprise, as the corporate in-house and cloud databases are classified as HBI assets. A high possibility of occurrence is justified by the fact that no technical controls are currently installed on the Smartphone devices and at the same time many kinds of exploit types can affect the devices (e.g. hacker attacks, viruses, spyware). The specific enterprise risk is rated as "High", since both its impact and its possibility to occur are high.

Another potential threat affecting the corporate data stored on the employee-owned devices is the unauthorized access to them in case of the Smartphone device being stolen or lost. This threat relates to the fact that the Smartphone devices are by nature vulnerable, due to their size and portability. Taking into account that the device might be switched-off or password-protected when idle, the exposure level of the locally stored corporate data is rated as "Medium". In addition, as we already discussed the locally stored corporate data are classified as a MBI asset, and therefore the overall impact in case of such threat occurrence is rated as "Medium". Finally, the possibility of the threat occurring is also subjectively assessed as "Medium", taking into account that employees try to be cautious and not misplace their devices, while also considering that a lost device may be retrieved by a benevolent person that will return it to its owner or deliver it to a police station. This enterprise risk is rated as "Medium", as both its impact and possibility are rated to be medium.

The complete results of the risk assessment stage can be found in Appendix D.

Key Information Risks										
	Asset		Exposure							
Risk ID	**Asset Name**	**Impact Class Rating**	**Defense-in-Depth Layer**	**Threat Description**	**Vulnerability Description**	**Exposure Rating (H,M,L)**	**Impact Rating (H,M,L)**	**Current Controls Description**	**Probability Rating w/Control (H,M,L)**	**Risk Rating w/Control (H,M,L)**
1.1	Internal/ enterprise cloud databases	HBI	Host	Disclosure/replication of corporate data through deliberately placed weaknesses on the Smartphone platform	Negligent employee deliberately overriding the enterprise security policies (e.g. via use of a jailbroken Smartphone, downloading applications from an untrusted app store)	M	M	Employee training on Smartphone BYOD policies including device protection best practices Background checks on employees	M	M
1.3	Internal/ enterprise cloud databases	HBI	Host	Unauthorized access to corporate data through theft of employee credentials	Theft of credentials off managed **remote client** due to lack of antivirus software or outdated	H	H	Employee training on Smartphone BYOD policies including device protection best practices	H	H

					security patches on the Smartphone device					
1.4	Internal/ enterprise cloud databases	HBI	Data	Unauthorized access to corporate data through theft of employee credentials	Theft of credentials via non technical means (e.g. eavesdropping, Social Engineering attacks)	H	H	Background checks on employees	L	M
1.7	Internal/ enterprise cloud databases	HBI	Network	Unauthorized access to local corporate data by a malicious person (e.g. via Back Door software, IP Spoofing)	Weak perimeter defense and data encryption mechanisms, lack of sufficient audit tools and host configuration	H	H	Password protection on the enterprise Wi-Fi network Intranet firewalls for monitoring incoming/ outgoing traffic Data at rest is encrypted via a standard encryption algorithm	H	H
2.1	Internal corporate databases	HBI	Network	Disclosure/ modification of corporate data in transit by a malicious person (e.g. Sniffing	Weak perimeter/ network protection mechanisms	H	H	Password protection on the enterprise Wi-Fi network Intranet firewalls for monitoring incoming/	H	H

				attacks, Man-in-the Middle attacks)				outgoing traffic		
2.2	Internal corporate databases	HBI	Application	Unauthorized access to the internal applications by a malicious person through Password attacks	Poor authentication mechanisms used for accessing the internal applications	H	H	Single-factor authentication using username-password pairs Employee training on protection/ regular updating of credentials	M	M
2.3	Internal corporate databases	HBI	Host	Unauthorized access to corporate data through theft of employee credentials	Theft of credentials off **local host** via outdated configuration of antivirus signatures, host configuration, or outdated security patches on the enterprise servers	H	H	Antivirus software installed on local servers/ workstations Intranet firewalls for monitoring incoming/ outgoing traffic Regular checks on available system updates and patches for the local hardware	H	H
3.1	External corporate databases on the Cloud	HBI	Application	Unauthorized access to the enterprise SaaS applications by a malicious person through	Poor authentication mechanisms used for accessing the SaaS	H	H	Reliance on the cloud vendor's authentication mechanisms	M	M

				Password attacks	applications					
4.3	Data centers/ Servers	HBI	Host	Interruption of business services due to flooding attacks on the enterprise servers	Lack of sufficient server security measures against High Load/ Denial-of-Service attacks	H	H	Standard backup/ recovery mechanisms Intranet firewalls for monitoring/ blocking heavy incoming traffic	H	H
9.1	Corporate data on employee smart phones	MBI	Data	Unauthorized access to corporate data stored on the device by a malicious person	Lack of security measures for cases of a device being lost/ stolen	M	M	No controls	M	M
10.1	Employee personal data	LBI	Data	Legal prosecution against the enterprise for violating employee privacy rights during Smartphone monitoring	Lack of appropriate legislation related to the protection of employee privacy	L	L	No controls	H	M

Table 6 – Key information risks for the system's most valuable assets

3.4 Conclusions

In this chapter, we developed a complete and correct design requirements checklist, by analyzing the security and legal aspect of Smartphone BYOD adoption. This list of requirements, presented in Table 3, is the answer to research question three. These identified requirements make up the logical architecture layer of our tailored SABSA model. The effectiveness of this logical security architecture should be supplemented by taking into account current information security risks that affect the enterprise's key assets. For this, we first provided a theoretical description on different risk assessment frameworks. Next, in paragraph 3.3.3, we implemented the most appropriate methodology for our enterprise-cloud system, in order to derive the list of the key indentified risks for the enterprise. Thus, this chapter has also provided the answer to the fourth research question, which was presented in Table 6.

The next chapter describes the Conducting Decision stage, during which a number of appropriate security controls is identified, evaluated and selected, in order to mitigate the information risks that were found in the Assessing Risk stage. Finally, a subset of these proposed controls, along with additional security mechanisms that fulfill the security architecture's legal and security requirements is deployed on the network to assemble our proposed component security architecture.

Chapter 4: Designing the Security Architecture

4.1 Decision support stage

Having developed the prioritized list of risks for the enterprise's most valuable assets, the next stage, which is known as Conducting Decision Support, relates to determining the appropriate actions in order to mitigate the aforementioned risks. During this stage, security controls are evaluated for their effectiveness, by estimating the degree of risk reduction that each control can provide (51). What is more, the security controls' cost efficiency is calculated via a cost-benefit analysis, to ensure that the costs for implementing, maintaining and monitoring a defense mechanism do not exceed the benefits that it offers to the corporation (59). Consequently, the enterprise's plans on treating each risk range from avoiding or mitigating it to transferring or even accepting it, depending on the cost-benefit analysis results.

Before considering the implementation of additional security controls, the enterprise's current security landscape is assessed, based on a Business Risk Profile (BRP) and a Defense-in-Depth Index (DiDI) as defined by the Microsoft Security Assessment tool. The Business Risk profile is a measure of the risk related to the industry and business model of enterprise, whereas the Defense-in-Depth Index relates to the current security defenses used across people, processes and technologies that can help in mitigating the identified security risks. In addition to the BRP and DiDI ratings, the security maturity of the organizations at stake is also measured, in order to assess the enterprises' ability to effectively make use of the strong security and maintenance practices that are currently available (51).

4.1.1 Theory on security control types

Security controls can be classified according to the plane of application in one of the following three areas of analysis: operational, organizational or technical. By operational controls we refer to the controls through which the handling of data, software and hardware can be secured. The environmental and physical protection measures are also part of the operational controls. Organizational controls refer to the formal procedures and processes, through which the duties of all actors related to the organization are defined. Technical controls relate to all complex technological components that constitute the organization's information systems. They include a system architecture design, hardware, software and firmware elements. Another way of categorizing security controls is based on their functionality. In this sense, security controls can be subdivided into the following three categories: preventive, detection and recovery controls. Preventive controls are the first controls that are met by an adversary and aim to eliminate a threat from occurring. Detection controls come into play when preventive controls have failed and their aim is to detect the occurrence of a

security violation. The function of recovery controls is to correct the situation or restore corporate information after a security violation has been detected (51). In this aspect, multiple layers of security controls should be combined, since any type of layer can be breached, regardless of the control's strength and reliability. According to the "defense in depth" principle, preventive controls should be in place to prevent security incidents from happening at all, whereas detection/recovery controls should also be installed to check whether the preventive mechanisms have been compromised and respond effectively to contain the damage (59).

The following section relates to the justification of our recommended actions, in accordance with a security control selection guideline based on industry standards. In this aspect, concrete reasoning on mitigation actions for a subset of the identified risks is provided. The same process was applied for all key identified risks, in order to derive the end results of the Decision Support stage that can be found in Appendix E. A list of all proposed security controls, along with their area-of-analysis and functionality classifications can be found in Appendix F. This list constitutes the physical architecture layer of our tailored SABSA model.

4.1.2 Recommended security controls guideline

The Recommended Security Controls for Federal Information Systems and Organizations is a guideline on selecting and specifying security controls for all information system components that process, store, or transmit corporate information. This guideline has been developed to help achieve more secure information systems and a more effective risk management. More specifically, the guideline provides a recommendation for minimum level information system security controls while offering a flexible security control catalog, through which organizations can meet current and future organizational protection needs, based on changing requirements and technologies (61).

According to the guideline, the control selection process can be broken down into the following three steps that are carried out sequentially: selecting the initial set of baseline security controls, tailoring the baseline security controls and supplementing the tailored baseline. As a starting point for the system's security, a selection of the initial set of security controls is carried out, based on the impact class of the relative enterprise assets, as it has been defined during the Assessing Risk stage. In this sense, the organization selects amongst three sets of baseline security controls provided by the guideline, which correspond to the low-impact, moderate-impact, or high-impact rating of an asset. Next, during the tailoring process, the selected baseline controls are modified and aligned with the enterprise's environment and processes, by specifying organization-defined parameters that make the implementation of the specified controls feasible. Finally, during the supplementation step, the tailored baseline is enhanced through the evaluation of threat and vulnerability information, risk tolerance levels and organizational policies that leads to the selection of additional security controls (61).

Figure 10 below illustrates an example for "Device Identification and Authentication" security control selection via the "Recommended Security Controls for Federal Information Systems and Organizations" guideline. The security control structure consists of five components: a control section, a supplemental guidance section, a control enhancements section, a references section and a priority and baseline allocation section (61).

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates [*Assignment: organization-defined list of specific and/or types of devices*] before establishing a connection.

Supplemental Guidance: The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for identification or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the security categorization of the information system.

Control Enhancements:

(1) The information system authenticates devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based.

Enhancement Supplemental Guidance: Remote network connection is any connection with a device communicating through an external network (e.g., the Internet). Related controls: AC-17, AC-18.

(2) The information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

(3) The organization standardizes, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to devices, and audits lease information when assigned to a device.

Enhancement Supplemental Guidance: With regard to dynamic address allocation for devices, DHCP-enabled clients typically obtain *leases* for IP addresses from DHCP servers.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** IA-3	**HIGH** IA-3

Figure 10 - Security control selection example. Source: (61)

The control section provides concise description of the security-related activities or actions that need to be carried out by the corporation or by the information system. Organizations can tailor the proposed security control to support their mission, business, or operational needs, thanks to the available degree of flexibility on parameters and input values of the control statement. The supplemental guidance section provides additional considerations related to the enterprise's environment,

mission and information risks, which should be taken into account while defining, developing, and implementing the control. The security control enhancements section provides statements of security capabilities that can build additional functionalities to a control or increase its strength. Such control enhancements are recommended for information systems requiring greater protection due to the higher impact of a threat occurrence. The references section provides a list of applicable legislations, directives and standards, as supporting information for the implementation of a particular security control or control enhancement. The priority and baseline allocation section provides the recommended priority codes for sequencing decisions, the baseline allocation of security controls and control enhancements for each asset impact class (61).

4.1.3 Justification on recommended control sets

Risk 2.3

The risk of employee credentials being stolen from local databases requires a number of actions for securing the enterprise environment, to prevent the leakage or modification of information that affects both its confidentiality and integrity (63). Due to the affected asset's high impact class, our proposed actions are based on the high baseline columns regarding the access control (AC), system and communications protection (SC) and system and information integrity (SI) suggested control families from the NIST guideline (61). The deployment of a perimeter network *(SC-7)* as a fundamental preventative control for the specific risk in not only in line with the "defense-in-depth" principle but also with the principle of compartmenization (57). This means that a DMZ segment creates an additional layer of security, as it constitutes an intermediary location between the organization's internal databases and the Internet. Consequently, the DMZ segment limits the damage to the critical compartments, since a successful attacker can only access the equipment in the perimeter network (58). Such a security control can be combined with preventive host-based firewalls *(AC-3)*, which should also be configured with highly restrictive rules to prevent any unauthorized access. The justification behind the deployment of intrusion detection systems *(SC-28)* is based on the enterprise's need for a detection control in the event of the aforementioned preventive mechanisms failing, which would lead to an attacker infiltrating the corporate internal network. In the same sense, antivirus solutions *(SI-3)* add a crucial security layer as a detection and recovery mechanism for attacks that have already reached the enterprise endpoints (servers and databases) (62).

Risk 4.2

The risk related to enterprise hardware being damaged by a malicious person can affect the availability attribute of the security architecture (e.g. damage to the enterprise servers would make business applications/processes unavailable to employees) (63). The suggested actions are based on the high baseline physical and environmental protection (PE) and awareness and training (AT) control families from the NIST guideline and involve the implementation of additional operational controls to the

current security measures installed in the corporate buildings (61). More specifically, apart from the standard locks and alarms, employee access cards, security guards and use of lockable cabinets should be the added preventative controls, whereas visitor logs can be kept as a detection control for the case of unauthorized people accessing the premises. *(PE-2), (PE-3)* The implementation of biometric access controls to the premises is too costly, despite offering a higher level of physical security, and therefore is not suggested, as it violates the cost efficiency principle (59). On top of the operational controls, the implementation of organizational controls related to employee awareness training *(AT-2), (AT-3)* is deemed necessary to reduce the chance of the risks' occurrence due to the "human error" factor (57). Such controls provide an additional preventive defense layer, since proper training can reduce the risk of negligent employee behavior (e.g. losing access cards, forgetting to lock cabinets etc) (61), (62).

Risk 9.1

In the event of an employee-owned Smartphone being stolen or lost, both the owner and the enterprise have no control on the device anymore. In such case, any malicious person obtaining the Smartphone could harm both the confidentiality and the integrity of both enterprise and personal information that is stored on the device, by disclosing or modifying them (63). The event of device theft or misplacement could occur when the employee is not on-premises and therefore no mechanism could eliminate this threat. Consequently, the suggested control, according to the moderate baseline of the media protection (MP) family from the NIST guideline, is to implement a remote lock or wipe of the device *(MP-6)*, which would protect unauthorized access or processing of confidential data (61). This preventative control is in line with the principle of failing securely, meaning that despite the chance of the device being retrieved, the default status of a lost Smartphone should be that it doesn't contain confidential information (57). The additional preventative controls of data encryption and PIN protection are suggested, in line with the moderate baseline of the device identification and authentication *(IA-3)* section of the NIST guideline, with an aim to prevent access to the corporate data on the devices, in the case that the Smartphone has not yet been reported as missing (61).

Risk 3.1

The risk of a malicious person accessing the enterprise cloud environment by exploiting the poor authentication mechanisms used for the SaaS applications can harm both the confidentiality and the integrity of the corporate data that is stored on the cloud through their disclosure or modification (63). Due to the asset's high impact class, our recommended action, based on the high baseline columns regarding the identification and authentication (IA) control family from the NIST guideline, is to transfer the authentication mechanism on-premises by implementing a single sign-on paradigm that is based on a trust relationship between an enterprise server and a corresponding federation server on the cloud environment *(IA-2), (IA-3)* (61). The reasoning on this specific authentication mechanism is based on the "don't trust services" and the

"minimization" principle (57). More specifically, since authentication is the main preventive technical control against unauthorized access of confidential information, it is better for the corporation to implement the mechanism in-house, rather than rely on the cloud vendor's defenses, which it cannot influence or control. What is more, by following the minimization principle, it is preferred that a single-sign on solution is implemented instead of having dedicated logins for each business application, due to the added complexity of the security system and the additional risks that derive from employees having to protect extended lists of credentials. Upon transferring the risk to the enterprise, a multi-factor authentication mechanism based on a what-you-have approach (e.g. via temporary codes sent via SMS to the Smartphone) is suggested *(IA-5)*, as the current simple password authentication mechanism does not provide adequate security. The additional policy requirements on more complex and limited-lifetime passwords *(IA-5)* constitute an additional preventative security control against password cracking attacks (61). Finally, the suggested technical control of applying alerts and thresholds on failed authentications *(IA-5)* is in line with the "defense-in-depth" principle that stresses the need for detection/recovery security layers for the event of all preventive controls' failure (57), (61).

Risk 1.2

The lack of strong authorization rules in the current authentication mechanism creates the risk of current employees accessing higher-level corporate data or applications that lie outside their duties. This sets both the confidentiality and the integrity of enterprise information at risk, since employees could modify or publish sensitive data (63). Our suggested action for the specific risk involves, according to the high baseline columns regarding the identification and authentication (IA), access control (AC), audit and accountability (AU) and personnel security (PS) control families from the NIST guideline, a combination of preventive and detection controls (61). More specifically, the suggested access control mechanism is a role-based approach that should be enforced in both database and application levels *(IA-2), (AC-2),* so that confidential information is still secure when the client application is exploited. The suggestion for a role-based access control (RBAC) is based on the fact that this approach provides an added layer to abstraction by assigning access permissions to roles than to individual users. A discretionary access control (DAC) mechanism is not preferred due to the fact that privileges are user defined and therefore data is prone to inappropriate permissions. On the other hand, a mandatory access control (MAC) mechanism lacks the flexibility of manual permission updates (e.g. for the case of employee job rotation or promotion), while the additional per-domain restrictions increase the level of complexity and the costs of implementation to an undesirable level (62). The suggested authorization mechanism is also in line with the "least privilege principle" *(AC-6),* since employees are granted access only to the data/services related to their roles and obligations (57). The logging across all applications *(AU-1), (AU-10)* is suggested as the detection control in the case of a failure in the authorization mechanism, in order to monitor failed and successful authentication attempts as well as modifications in sensitive data (57), (62). Finally, the organizational control of performing background checks on employees *(PS-*

6) is aimed to prevent the employees from attempting to act maliciously. In this aspect, the risk can be prevented if the firm's managers dismiss or not hire at the first place suspicious personnel (61). Such organizational controls are crucial due to the "human error" factor of the specific threat.

Risk 1.3

Next the risk of a malicious person obtaining employee credentials through a Smartphone host is addressed. In such an event, both the integrity and confidentiality of corporate data can be harmed, as the malicious person can disclose, replicate or modify information upon gaining access (63). Because the ownership of Smartphone devices lies on the employee side, enterprises cannot rely on them for implementing security mechanisms, since they cannot be aware of the security mechanisms that they will be willing to deploy. Due to the high impact class of corporate data, the suggested actions are derived from the high baseline access control (AC), identification and authentication (IA), system and communications protection (SC), media protection (MP), audit and accountability (AU) and planning (PL) control families from the NIST guideline (61). Therefore, the recommended action is to deploy a Mobile Device Management (MDM) system within the enterprise network, through which enterprises can distribute and manage preventive, detection and recovery tools on the employ-owned devices *(MP-5), (IA-3).* The reasoning behind this action can be explained via the "weakest link" principle (57). This means that an enterprise should install security controls on the smart phones that are currently lacking any defense mechanisms and are therefore exposed to malicious attacks. The preventative controls that should be distributed via the MDM server are critical updates and patches *(SC-28)* so that all known software weaknesses have been covered (62). What is more, the MDM server allows the audit of smart phones *(AU-1),* which is required in order to ensure that employees have applied restrictions on the phone's software and hardware features. The enterprise should formulate a formal acceptable-use policy *(AC-1), (PL-2),* where the permitted protocols, applications and sensors are defined, so that restrictions on smart phones are universal for all employees in the firm. The organizational control of monitoring/managing the devices is deemed necessary in order to eliminate the "human error" factor, since negligent or malicious employees might install applications or enable features that are vulnerable to virus or malware attacks (57). Finally, the installation of anti-virus and anti-malware clients on the smart phones via the MDM system *(SC-28),* as the detection and recovery controls for the specific risk, is justified due to the chance of the aforementioned preventive mechanisms failing (e.g. because hackers continuously trace new weaknesses or gaps in operating systems and applications) (62).

Risk 10.1

The risk of legal prosecution against the enterprise for violating its employees' privacy rights during the monitoring of the Smartphone devices affects the confidentiality and integrity of personal information stored on these devices (63). This risk relates to the company's compliance to the legal rights of mobile employees. Threats affecting the

employee personal data have minimum direct impact on the enterprise's processes. Nevertheless, potential legal prosecutions can still indirectly harm the enterprise's business. Consequently, the suggested action, according to the minimum baseline audit and accountability (AU) and media protection (MP) control families from the NIST guideline, is to implement organizational controls to ensure employee data privacy (61). More specifically, the suggested preventive control is a formal signed contract between the employer and an employee, with the employer consenting to allow usage of employee-owned smart phones at work and the employee allowing the corporation a specified level of access to the device the personal data stored in it *(MP-2), (AU-2), (AU-3)* (47). In addition, a regular monitoring of the enterprise security processes by and independent third party *(AU-1)* is suggested as a detective mechanism for any deviations from the legal contract (60).

4.2 Component security architecture proposal

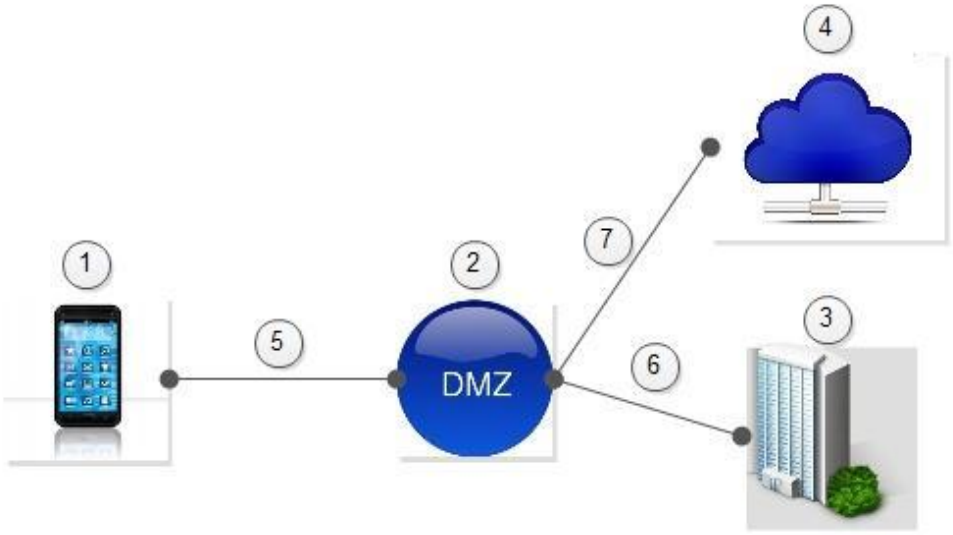

Figure 11 – System topology

Having described the physical architecture layer of our customized SABSA model, which comprises the security mechanisms that meet the design requirements, we assemble in this section our proposed component architecture, where specific security components are precisely positioned in the system at stake. The system consists of the Smartphone devices, the corporate perimeter and internal network and the enterprise Cloud, as well as the communication channels between the different locations, as Figure 11 depicts. However, no technical security controls are deployed on the cloud environment, since the SaaS model requires that the cloud vendor maintains control of all security aspects of the cloud (19). It should be noted that not all possible recommended controls were implemented, since such an approach would not be cost-efficient. The deployment of technical components on both the remote client and the enterprise network is realized in the way that satisfies the identified security and legal requirements of the security

architecture (see Table 3), as illustrated in Table 7, below. The reasoning on the location deployment for each technical component is elaborated in section 4.2.1.

Topology location (Fig. 11)	Design requirement fulfilled (Table 3)	Security Control	NIST Control Code (61)
1. Smartphone Platform	2.b.	Encrypt Data at-rest in device and external storage spaces	SC-28
1. Smartphone Platform	1.d. 2.b.	Apply Device PIN-lock	IA-3
1. Smartphone Platform	2.b. 2.d.	Deploy mobile anti-virus and anti-malware software via the MDM client	SI-3 SC-28
2. DMZ zone	2.a. 2.e.	Route all traffic through the external firewall	SC-7 AC-3
2. DMZ zone	2.a.	Deploy network-based IDS at the entry point	SC-7 SI-4
2. DMZ zone	2.e.	Deploy reverse-proxy gateway servers to authenticate access to the VPN tunnel for secure remote device access towards the enterprise and cloud servers	SC-7 CA-3
2. DMZ zone	2.c.	Deploy load balancers to ensure availability of the gateway servers	CA-3
2. DMZ zone	2.a.	Deploy enterprise web servers on the DMZ zone to separate from the internal critical servers/databases	SC-7
2. DMZ zone	1.c.	Deploy a proxy server to limit normal internet access of remote workers to trusted websites/apps	SC-7 CA-3
3. Enterprise intranet	2.a. 2.e.	Route all traffic through the enterprise firewall	AC-3
3. Enterprise intranet	2.a.	Deploy network-based IDS at the entry point	SI-4
3. Enterprise intranet	2.e.	Deploy a ticket granting system for SSO authentication	IA-3 IA-5

3. Enterprise intranet	1.c. 1.d. 2.b. 2.e	Deploy MDM management servers through which instructions are sent to smart phones for: Enrolling/Un-enrolling a device to/from the Active Directory, remote locking/wiping, disabling of sensors/cut-paste commands, defining website/application permissions on the web proxy	IA-5 SC-9 SC-18 AC-17 MP-5
3. Enterprise intranet	1.b.	Enable logging of all device monitoring activities that access/process employee personal data on smart phones	AU-12 SI-4
3. Enterprise intranet	2.c.	Deploy load balancers to ensure availability of the MDM management servers	CA-3
3. Enterprise intranet	2.a. 2.c.	Deploy anti-virus and anti-malware software on all corporate servers	SI-3 SC-28
3. Enterprise intranet	2.a.	Deploy host-based IDS on the LOB application servers to protect from back-door exploitations	SI-4
3. Enterprise intranet	2.f.	Enable logging of user-access and data processing on the application level	AC-7 AU-12
3. Enterprise intranet	2.a.	Encrypt Data at-rest in local databases	SC-28
3. Enterprise intranet	2.f.	Enable logging of user-access and data processing on the database level	AU-12 SI-4
4. Enterprise cloud	2.e.	Establish federation trust for on-premise SSO authentication based on ticket granting	IA-2 IA-3
5. Smartphone – DMZ communication	2.a. 2.f.	VPN tunnel with data in-transit encryption	AC-17 SC-8
6. DMZ – Intranet environment communication	2.a. 2.f.	Data in-transit encryption	AC-17 SC-8
7. DMZ – Cloud environment communication	2.a. 2.f.	Data in-transit encryption	AC-17 SC-8

Table 7 - Overview of the artifact's technical components

4.2.1 Deployment of selected technical controls

The deployment of our selected technical security controls is carried out in a way that complies with the Recommended Security Controls for Federal Information Systems and Organizations guideline, which aims to protect the prioritized assets, as they were classified in Table 5. In this sense, each selected security control is appropriately deployed to reduce the asset's vulnerability to the internal or external threats that could compromise the artifact's security and legal requirements. The detailed implementation process is described in this section.

A Mobile Device Management (MDM) server should be deployed within the enterprise network, so that it can provide IT managers with an administrative control, through which the mobile MDM clients can distributed, maintained and supported in the employee-owned remote hosts (37), (57). The MDM server enables the enrollment of Smartphone devices in the enterprise environment, the distribution of certificates and the application of device configurations according to the company's security policies (35) (41).

As it has already been justified in section 4.1.3, a DMZ zone should be deployed outside the enterprise intranet, in order to separate the critical enterprise servers. According to the NIST guideline, the enterprise web servers should be moved on the DMZ location in order to protect the LOB application and database servers in the event of a successful intrusion (61). Two different hosts are deployed on the perimeter network. First, an MDM gateway server is used to secure the communication of registered Smartphone devices with the enterprise resources. More specifically, the MDM gateway is a reverse proxy server that accepts incoming Smartphone connections and then connects to enterprise cloud and in-house destination servers. In this sense, the MDM gateway can be configured to limit access to specific hosts and to encrypt data transfers based on certain protocols (e.g. by deploying a reverse proxy with SSL acceleration hardware) (62). What is more, a forward proxy server is deployed in the perimeter network, through which Smartphone access for permitted Internet locations is re-routed. Both proxy servers should be deployed at the DMZ zone, because they both are intermediary servers that regulate the traffic towards the enterprise-cloud network and the permitted Internet locations respectively (61).

According to the NIST guideline, the recommended firewalls should be installed at the DMZ and intranet entry points in order to create choke points for all incoming and outgoing traffic (61). In this way, the enterprise and DMZ environments' vulnerability to unauthorized entry can be reduced, by defining highly restrictive rules for the firewalls. At the same time, network-based intrusion detection systems should be deployed next to the DMZ and corporate firewalls, as this way unauthorized users as well as Denial-of-Service (DoS) attacks are timely detected before reaching the enterprise servers (61), (62). Additional host-based intrusion detection systems should be implemented on the in-house LOB servers, as in this location the host-based IDS systems can readily "see" the intended outcome of attempted attacks, due to them having real-time access to the critical files and processes that attackers try to target (62).

Since the role of load balancers is to distribute the workloads across the corporate resources and thus maximize throughput, they should be deployed in front of the MDM gateway and MDM management servers, which are the enterprise's most critical resources as they receive, authenticate and manage all traffic towards the rest of the in-house and cloud servers (61). In this way, the load balancers reduce the servers' vulnerability to Denial-of-Service attacks and ensure higher availability in cases of high access demand. At the same time, they prevent clients from directly contacting the backend MDM gateway and management servers, which could jeopardize the kernel's network stack by exposing the internal network structure (58).

The guideline's recommended authentication mechanism should be based on a single sign-on, multifactor approach for both local and remote users (61). Consequently, the authentication of external devices should be realized via the MDM gateway server, which communicates with the in-house authentication/ticket granting system via the centralized MDM management server, in order to prevent direct access to the enterprise Intranet (30), (34), (37). The active directory containing the employee credentials should still be deployed in the secured intranet (61). A trust relationship should be established between the corporate authentication server and a corresponding federation server, which is located on the SaaS provider's network (39). In this way, the design requirement for integrated cloud authentication is fulfilled, since remote device access to the enterprise SaaS applications is established through the use of signed security tokens upon successful negotiation between the cloud federation and the internal ticket-granting servers (30), (43).

The authorization and access control mechanism should also be enforced and managed internally, via the MDM management server (37). As we already justified in section 4.1.3, role-based access controls are enforced for both the database level and the application interface, since in this way IT managers can limit both the access to all corporate resources and the installation of mobile applications depending on the user's role within the enterprise (36), (62). Additional restrictive rules are applied on jailbroken/routed smart phones, since these devices can be easily compromised and should therefore be restricted from the corporate network.

Due to the fact that the access of corporate resources takes place through wireless communication that is vulnerable to interceptions by both malicious outsiders and insiders, as we already elaborated in the risk assessment output (Appendix D), the NIST guideline indicates that all traffic from the Smartphone's 3/4G or its Wi-Fi connection should be totally encrypted in order to secure the HBI corporate asset (i.e. all corporate and cloud databases) (61). For this, a VPN tunnel should be established to secure incoming traffic from untrusted locations/devices over the Internet, as it supports data-in-transit encryption protocols (such as IP Security (IPSec), Secure Sockets Layer (SSL), and Secure Shell (SSH) technologies) (34), (36), (37). The reverse proxy gateway server can serve as the endpoint of the VPN tunnel, while it assists in limiting data exchange within the intranet and cloud locations in a secure way (61).

According to the NIST guideline all data-rest locations should be encrypted using strong public key encryption schemes (such as 3DES or AES algorithms). Consequently, the suggested measure of encrypting data residing in both the corporate databases and the Smartphone local and external storage is in line with the guideline's point on reducing the data vulnerability to unauthorized access/modification (61), (62).

The malicious code protection (SI-3) section of the NIST guideline indicates that anti-virus and anti-malware solutions should be used as fundamental tools for detecting and responding to viruses, worms and spyware software respectively (61). Due to fact that such threats affect the operating system and application layers of computing systems, this anti-virus and anti-malware software should be deployed throughout the environment on both servers and workstation to effectively detect and eliminate viruses and other types of malicious code (61), (62). At the same time, mobile anti-virus/anti-malware clients, along with any critical software updates and patches for the MDM agents, should be pushed on the Smartphone devices to protect. Such software can be actively managed via the in-house MDM management server (35) (61).

The remote locking/wiping of smart phones, in order to prevent corporate data leakage in the case of a device being lost relates to the media protection (MP) and remote access (AC-17) sections of the NIST guidelines (61). According to the guideline, the locking and wiping should be controlled from an administrative internal server that IT managers have access to, and is therefore managed by the internal MDM server (35). In more detail, IT managers can remotely lock Smartphone devices by transmitting a remote lock or data wipe command message using the remote control module on the MDM device management server to the specific Smartphone. The command-processing module of the MDM agent running on the Smartphone receives the control command via an SMS notification message and locks the Smartphone with a pre-defined password set by the IT management board or deletes the user data on the Smartphone respectively (38), (42).

As far as the audit and system integrity tools are concerned, the NIST guideline directs to enable logging both at the LOB application servers and at the internal database servers, so that unauthorized changes in confidential data can be tracked both during their processing and storage. At the same time, log files should be generated on the internal authentication/ticket-granting server to monitor authentication attempts from unauthorized or malicious users (61). Finally, due to the employee data privacy legislation that enterprises should comply with, log files should be generated on the MDM management server for transparent Smartphone monitoring (47).

The composition of all aforementioned technical components constitutes the proposed component security architecture, which is illustrated in Figure 12. However, the enterprise's reliance on technical controls alone is insufficient without complementary organizational and operational controls (62). Due to the fact that organizational and operational controls are not visible in the security architecture figure, these control sets are elaborated next, in sections 4.2.2 and 4.2.3 respectively.

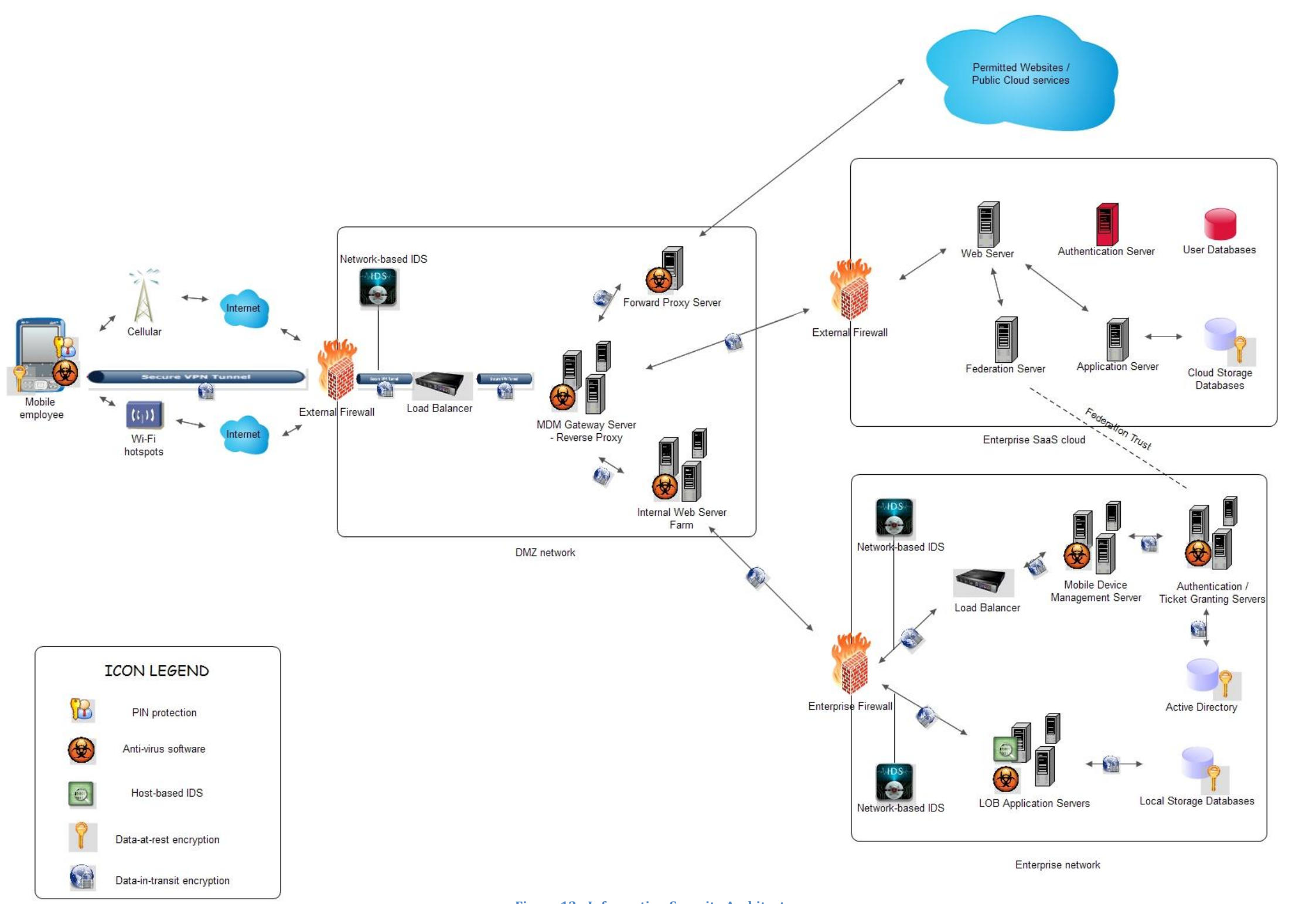

Figure 12 - Information Security Architecture

4.2.2 Analysis of operational controls

The preventative operational controls of our proposed security architecture include electronic locks, fences and security guards that protect the enterprise facilities from intruders. Additional locks for employee workstations and alarm systems are also deployed to further secure the computing facilities. What is more, automated fire protection systems and temperature/humidity control systems should also be installed in order to protect the organization's key assets from natural disasters. Emergency backup power for sensitive electrical systems should be available, so that applications and operating systems are shut down in a gracefully manner in cases of power brownouts and blackouts. Backups of critical media should be stored offsite to facilitate the restoration of lost or corrupted data in the event of a catastrophic incident. In order to preserve the enterprise data, formal disposal procedures should be followed to ensure that the Smartphone external storage devices along with replaced enterprise hardware are rendered unreadable by degaussing or other methods before disposal (59), (62).

As far as the detection and recovery controls are concerned, security guards along with the installation of surveillance cameras, motion/flood detectors and alarm systems play a dual role of both detecting and preventing the organization from attackers and environmental threats (51).

4.2.3 Analysis of organizational controls

The preventative controls are mainly a number of documented security plans that explain how the different security components are installed and how the security processes are carried out. More specifically, the tasks that managers and employees will undertake when implementing the different security controls is defined in a formal documentation of roles and responsibilities (60). Such a documentation should be followed by a signed contract between the employer and the employees, so that consent for personal device usage and activity monitoring respectively can be established, thus fulfilling design requirement *(1.a)* as defined in Table 3 (47).

Our proposed security solution requires that an acceptable-use policy for employee-owned smart phones exists in the enterprise. In this sense, IT security and business teams should jointly establish and document guidelines for allowed protocols and services that can be installed on the employee devices. The policy should be periodically reviewed and updated to reflect new Smartphone technologies and environment changes (60).

Another preventative control that is part of our security architecture is the system for provisioning and de-provisioning users. The implementation of such system involves the prompt granting of access to corporate information for new employees and the disabling of terminated staff accounts in a timely manner, so that former employees are restricted from accessing enterprise resources. The provisioning processes should also include rules for employees that are transferred within the company to positions with a

different access level. In this sense, the provisioning system should define a clear separation of duties and privileges for employees so that they can utilize only resources that relate to their job tasks (60), (62).

Formal policies and procedures for governing the relationship with the external cloud partner should also be documented to fulfill design requirements *(1.e)* and *(1.f)* as defined in Table 3, thus preventing risk of exposure. The policies should define the partner's level of connectivity and access to the corporate network, the storage and manipulation of specific types of company data on the cloud environment and the definition of firm's processes that can be outsourced. Additional procedures that require deletion of all data remanence from the cloud should be included (27), (60).

The aforementioned procedures are realized through the technical controls that relate to the authentication and authorization of users in the enterprise network, which were elaborated in section 4.2.1.

Finally, the security awareness training is a preventative control that should be mandatory for all new members of the organization as part of the employee orientation program. All aspects of security should be covered, including security policies, network security, application security, physical security and personal Smartphone protection practices. Clear guidelines should be provided for what employees should do if they witness things that appear to jeopardize the security of any of these elements. Moreover, periodic testing should be implemented to ensure employees have absorbed the material, whereas updates and refresher courses should be regularly conducted to ensure all employees are aware of the most current practices and risks (60), (61).

The proposed detection controls relate to performing continuing reviews of the controls that are currently in place, in order to verify the system's efficacy. In this sense, our solution requires that a recurrent risk management program is in place, so that enterprises can mitigate new risks that may arise in the enterprise environment. Regular assessments of the infrastructure, applications, policies, and audit procedures should be conducted to gain an objective view of the firm's security posture. Employee smart phones should also be assessed to ensure that the devices are properly configured according to the firm's acceptable use policies. All security assessments performed by internal staff should be augmented with input from a trusted third party (59).

Detection controls related to the firm's workforce that should be included in our proposed artifact are background investigations on both potential and current employees, including reviews of the candidate's employment and legal history, in order to identify any potential issues that could put the organization at risk. In the case of promoting employees to positions that involve greater responsibility, more thorough checks should be performed, since such positions entail higher access levels in the corporate resources. Finally, the enforcement of duty rotation for mid-level employees is strongly encouraged, as it can be a means of detecting nefarious activities (51).

As far as the recovery controls are concerned, the proposed security solution should include a formal incident response and reporting planning, through which the enterprise's reaction and recovery from a security breach can be within an acceptable timeframe, while the incident is restrained from spreading to other corporate systems. The company should designate an emergency response team that includes representatives from several disciplines including technology, human resources and legal, for responding to all security incidents and issues. In addition, the enterprise should work on formulating up-to-date disaster recovery and business continuity plans that relate to the recovery from catastrophic events that affect a large fraction of the firm's IT infrastructure. Such plans should cover the entire technical, physical and staff environment and should be regularly tested to validate correctness and completeness (62).

4.3 Conclusions

In this chapter the proposed component security architecture has been designed. This was done by performing several sub steps. First, the Decision Support Stage was carried out, which provided us with recommended mitigation actions on the key information risks, as they were identified in the previous chapter. Thus, this stage described the physical architecture of our customized SABSA model. Next, a subset of the recommended controls set was selected and precisely deployed on the enterprise-cloud environment following a formal guideline based on industry standards, so that the proposed artifact is both effective and cost-efficient. The implementation of technical components was supplemented by necessary operational and organizational controls, in order to cover the physical and human-factor security aspects of our design. The target component architecture layer of our customized SABSA model was elaborated and illustrated in paragraph 4.2 and provides the answer to the fifth research question.

In the next chapter the proposed security architecture is checked for its validity through the communication with experts in the fields of cloud computing and enterprise mobility policies.

Chapter 5: Design Validation

In this chapter, the validation of the proposed security architecture is carried out. In this sense, we determine the degree to which our model is an accurate representation of the real world as far as the intended functions of the model are concerned. Furthermore, we examine to what extend our model meets the identified security and legal requirements. The utter goal of the validation stage is to make the proposed model useful in terms of addressing the correct problem and providing accurate and sufficient information on the designed artifact itself. For this, we first describe in section 5.1 the preparation steps that relate to how the expert panel was selected and how the validation process was structured. Next, we define the validation criteria, on which experts should provide their personal insight and feedback. In section 5.3 we elaborate on the results of the validation stage. Last, the conclusions on this chapter are presented in section 5.4

5.1 Validation set up

This section describes the process of expert panel selection as well as the preparation steps before conducting the validation stage. Since the experts were asked to evaluate both the selected components that constitute the security architecture and the processes we followed to derive the proposed artifact, we first needed to define a list of validation criteria related to our final design and the different methodologies we used. Besides assessing the artifact on these predefined criteria, the respondents were also asked to give recommendations that can improve the security architecture in terms of effectiveness, cost-efficiency, and feasibility. Depending on their availability, the respondents were reached either via videoconference for a short interview or via e-mail communication. As a pre-step, we provided them via e-mail with a summary document that describes the security artifact and its components, as well as the design steps that we followed during our research. In addition, the respondents were provided with our selected validation criteria list in order to be prepared for the interview. In some cases, the complete research document was also emailed to the respondents due to their interest in knowing the full extent of our research and findings. During the interviews the assessments of the experts were discussed while further clarifications were given whenever it was deemed necessary.

Regarding the process of selecting the experts that validated the proposed security architecture, we selected people with different competencies and job levels in order to broaden the scope of the validation process. More specifically, our expert panel consisted of the following three persons: mr. Wilco van Ginkel, who is currently working as a Senior Strategist at Verizon Business and his tasks relate to cloud security and cloud business development, mr. Rizwan Ahmad, who is the founder and CEO of the Cloud Security Alliance (CSA) New Zealand Chapter and mr. Kostas Pentikousis, who is currently working as a Senior Research Engineer at Huawei Technologies and his tasks relate to mobile networking and mobility management. In this sense, our validation group involved experts in both the cloud-computing field and in BYOD policies. What is

more, all selected experts have relative academic background in risk assessment and risk management, while they have real-life experience on applying such frameworks due to their job position requirements. It should be noticed here, that the experts were not involved in the design process of our security architecture. Each expert validated the framework based on his own knowledge and provided us with invaluable feedback in order to refine our proposed design. In the following section, the criteria on which the selected expert panel validated our security artifact are elaborated.

5.2 Validation criteria

In this section, the validation criteria, as they were defined before the execution of the expert validation stage, are discussed in detail. The criteria are selected based on the suggested guidelines of different risk management frameworks, in order to ensure that they are generally accepted and that they are relevant for the case of an enterprise adopting mobility policies.

Our first validation criterion is correctness/relevance. In this sense, our respondents were asked to evaluate whether the design requirements and the information risks that were identified relate to the case of enterprises adopting Smartphone BYOD and cloud technologies. The correctness of the security controls that were suggested to secure the adoption of such technologies is crucial, since the deployment of an improper security control for mitigating an information risk would lead to an unwanted outcome for the enterprise. Furthermore, correctness relates to the accepted level of residual risk. This means that the acceptance of a risk that was misidentified to have a low overall impact could have devastating results for the enterprise's business processes.

Another criterion that we used for the validation process is design completeness. This criterion relates to assessing the proposed design on the degree that it fulfills its intended purpose. In this sense, the experts were requested to evaluate whether our artifact fulfills all security and legal design requirements, which would imply that our main research objective has been met.

The usability of our proposed security artifact is our third criterion. In this sense, our expert panel was asked to evaluate whether our control implementation along with the risk assessment and design steps are communicated in a clear way, so that the target audience (mainly IT board of enterprises) has a clear view on what the relative risks in adopting Smartphone BYOD policies are and an understandable guideline on how the security controls should be deployed to mitigate these risks.

Our final criterion is flexibility of the proposed design. More specifically, the expert panel was asked to assess the flexibility of the design requirements' and information risks' identification processes, so that the design can be tailored for different types of enterprises. The flexibility of the control implementation was also assessed, in order to evaluate whether the proposed design can be adapted to newly emerged technologies that might entail additional threats (e.g. new smart phones with different operating

systems and features) and to different needs from both the employer's and the employees' side (e.g. need for more freedom on personal service access via the Smartphone devices).

5.3 Validation results

The experts' comments on the correctness and completeness of the design steps that we followed were overall positive. More specifically, the interviewees confirmed that the selected frameworks and industry standards are applicable to our enterprise-cloud system. Whereas the identified design requirements, against which our system was tested and measured covered all necessary aspects according to the experts, one recommendation was to formally justify our selection by using a formal guide, such as the NIST Security Self-Assessment Guide for Information Technology Systems, which provides an extensive list of design requirements that can be found in statute, policy, and guidance on security and privacy.

The ease-of-use level of our design was commented to be satisfactory, followed with an additional recommendation of extra figures that visualize some processes (e.g. in the risk assessment methodology comparison section).

As far as our design processes' flexibility is concerned, the only drawback that was indicated was that our design might not be easily adaptable to Non-EU based enterprises due to the different applicable data protection legislations. Nevertheless, such feedback was expected, as it was our intention to limit the geographical scope of our research.

Regarding the proposed final design, the experts pointed out a trade-off between flexibility and completeness of our artifact. In this sense, whereas our proposed security architecture can easily be adapted for different enterprises according to their preferences on application, social networking and device feature permissions, our solution does not describe a strict acceptable-use policy; it rather provides a guideline on what issues IT managers need to take into consideration before allowing the use of employee-owned smart phones for business purposes. Our suggested technical components however, enable the implementation of device restrictions and the secure transmission of corporate information towards and from the Smartphone devices, based on our complete mobile device management system.

The expert panel also indicated that the completeness of the proposed design also relates to the active participation and cooperation of the end-users (i.e. remote employees) in all phases. This factor was confirmed as satisfied in our design, as the proposed security architecture incorporates both the employee requirements in enabling the use of Smartphone devices for personal services (although the permitted external website/app list is limited) and the organizational controls relating to employee awareness/training on how to comply the enterprise security policies.

The technical components that we suggested were positively evaluated, as they correspond to current technologies that are used across enterprises using SaaS clouds and remote work polices, according to the experts' work experience. One recommendation from the technical perspective was to create a 2-tier perimeter network an/or a 2-tier enterprise intranet for added security, by separating the gateways from the web server farm or the application servers from the intranet databases respectively, and then deploy additional network-based firewalls at the entry points of the new segments.

One expert's comment on the viability of the proposed artifact however, was that the additional assets and technological components that are required in our design might be cost-prohibitive for micro entities and small enterprises (up to 50 employees). He suggested that such businesses could alternatively outsource the overall device management to a cloud vendor. This approach, despite being less secure, due to the uncertainty involved in external collaborations, is less costly thanks to a per-device renting plan.

From a non-technical approach on our final design, whereas the our proposed security architecture was commented as correct and up-to-date, the expert panel suggested that, according to industry-based good security practices, the risk assessment process should be scheduled at least every 3 years in an enterprise's system development lifecycle. However, this recommended schedule for assessing and mitigating key information risks should be flexible itself, in order to adapt to disruptive technological innovations into the IT system and updated applicable legislations and policies.

5.4 Conclusions

In this chapter, we defined how our proposed security architecture should be validated. In this sense, we described the preparation steps and the criteria on which a selected panel of experts would validate our design. Finally, the main remarks of the experts during the validation interviews were elaborated. This chapter has provided the answer to the sixth research question.

In the following conclusive chapter, we elaborate on the degree that our research contributes in the academic and industry fields. Next we present the limitations that restrain the generalization of our proposed security architecture for global enterprises. Finally some future research points that could improve the approach of securing Smartphone BYOD policies are discussed.

Chapter 6: Conclusions, Discussion and Future Work

6.1 Reflections on research questions and objective

As discussed throughout this report, the adoption of mobility policies and SaaS clouds introduces multiple risks for enterprises. This Master Thesis research proposes a security architecture design based on a customized application of the SABSA model. In this sense, we presented in our research multiple views and dimensions of the security architecture, starting with the contextual architecture that describes the enterprise business processes. From this information we derived with the logical design requirements that constitute the logical architecture, which was followed by a description of security mechanisms that meet the design requirements that make up the physical architecture. From this point we deployed a number of security components in the system at stake, in order to mitigate the enterprise risks to an acceptable level. The composition of the suggested technical, operational and organizational controls constitutes the component architecture, which was accompanied by the description of the service management architecture, where the maintenance processes for the proposed architecture were elaborated. Thus, this holistic approach on the proposed security architecture is the answer to our main research question:

"What enterprise security architecture can secure the access of SaaS cloud services by Smartphone BYOD?"

This question is answered by combining the answers to the research sub questions as they were defined in chapter 1. More specifically, we defined in Chapter 2 the business processes and the underlying IT infrastructure in an enterprise-cloud system, in order to answer research questions 1 and 2. Next we analyzed the legal and security requirements that our proposed security architecture should fulfill in order to secure the adoption of Smartphone BYOD and SaaS clouds. The design requirements were refined and enhanced by conducting a risk assessment, so that the relative information risks for our enterprise-cloud system could be identified. Consequently, we provided in Chapter 3 the answers to research questions 3 and 4. The risk assessment was conducted based on a qualitative methodology, whereas the identification of relative assets, threats and vulnerabilities was based on fictitious, extensive lists that are provided by industry standards and tools. In this sense, the answer to the fourth research question is partly limited due to the lack of real-life factor considerations. However, with this approach the applicability of our proposed security architecture can be generalized to enterprises from all business domains, provided that the identified risks will be first tailored according to each enterprise's business environment. In Chapter 4 we used a tool based on industry standards, in order to define the appropriate security controls that can mitigate the identified risks. Then in section 4.2 we presented our proposed design, which consists of a number of technical, operational and

organizational controls. We elaborated on the deployment locations for the suggested technical controls and we explained in Table 7 which design requirements are fulfilled by each technical control. Upon answering research question 5, we validated our proposed design with the help of experts in the fields of cloud computing and mobility policies, thus answering research question 6. The expert panel validated the proposed security architecture on the following validation criteria: Correctness, Completeness, Usability and Flexibility. Our design was assessed with positive scores on all criteria, as both the identified requirements and the suggested controls are relevant for enterprises adopting cloud technologies and BYOD policies. A tradeoff between the flexibility and usability of the design was indicated by the experts, who explained that our design can be applied to different types of enterprises, but it should be adapted to each enterprise's specific needs prior to its implementation. The combination of all six sub research questions provides the answer to the main research question and consequently fulfills our research objective of proposing:

"An enterprise security architecture that treats the information security risks induced by Smartphone BYOD accessing SaaS cloud services".

6.2 Scientific and practical contribution

Our research has both an academic and a practical relevance and therefore provides valuable input for both fields. In this section we discuss some opportunities that our research creates.

As we already mentioned in our introduction chapter, no tailored security solution exists that can be applied for enterprises adopting SaaS clouds and Smartphone BYOD policies, despite the need of managers to ensure that the integration of such technologies will not harm the enterprise mission and its business processes. Through our proposed design this practical gap is closed.

Our risk assessment and decision support approach can also contribute in relative enterprises' risk management strategies. In this sense, our research provides an overview of relevant risks and contemporary security methods, and can be therefore useful for the on-going process of risk management in companies that already implement mobility policies.

Finally, by taking into consideration the feedback received by the experts in cloud and mobile technology fields, different enterprises can increase their knowledge base by combining the different insights. This could facilitate in creating synergy amongst the numerous enterprises, which leads to more effective collaborations and partnerships between different players in the market.

However, the aforementioned benefits of our suggested design are limited, due to the variations in the different enterprise environments that require our solution to be adapted according to the relative stakeholders, regulations and technologies. In the next

section such design limitations are further discussed.

6.3 Design limitations

An important factor that limits the span of our research is the ever-changing enterprise environment itself. Over time, the corporations' customer network can expand, whereas the architecture components and the applications used for the business processes are updated, following contemporary technological advancements and trends. What is more, personnel changes will occur along with the enterprise business plans, which will also affect the security policies that need to be in place. All these changes imply the emergence of new information risks, together with the need of adapting previously mitigated risks to the changed enterprise environment. Consequently, despite our proposed security architecture's current level of effectiveness, an ongoing and evolving risk management strategy should be carried out to maintain a secure approach on mobility policies.

As it has already been discussed in our risk assessment chapter, the elimination of all risk is close to impossible. Consequently, the overall security of our proposed design is limited, as our selected set of technical, operational and organizational controls was based on a cost-efficient approach. In this sense the reasoning behind our selected controls relates to our aim to decrease the overall mission risk to an acceptable level while having minimal adverse impact on the enterprises' resources. Still, the presence of residual risk, although inevitable, poses another limitation for our research. The accepted level of a residual risk is explained through our risk mitigation plan, as illustrated in Figure 13.

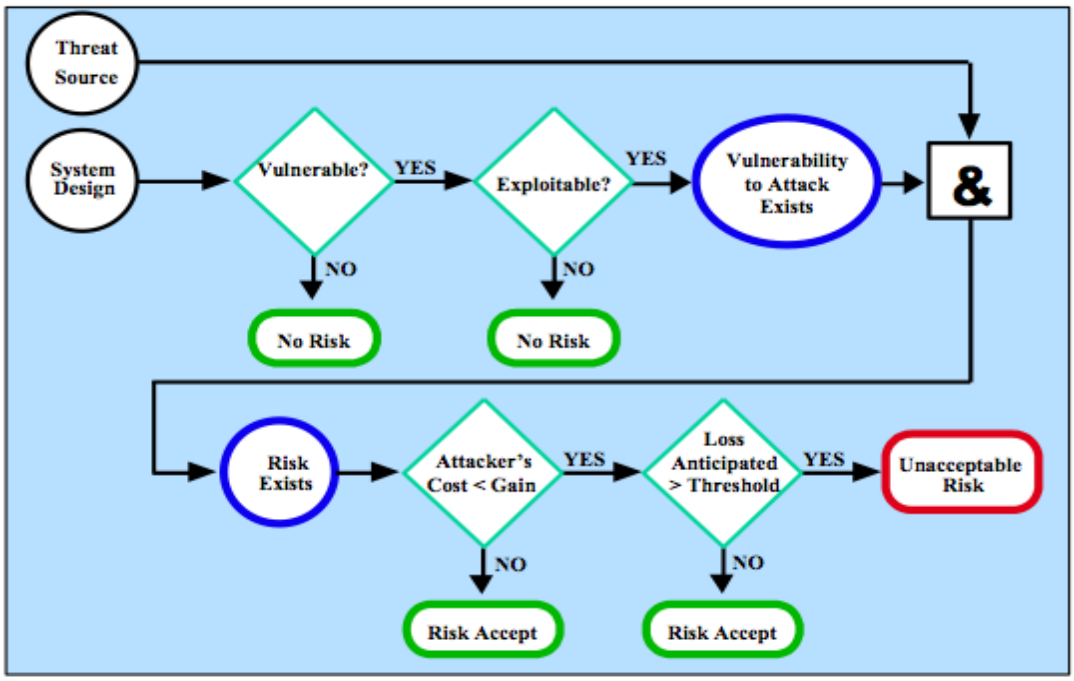

Figure 13 - Risk mitigation plan. Source: (59)

According to Figure 13, the appropriate points for implementing security controls are located on the "Unacceptable Risk" field. The residual risks that can still hinder the enterprise business processes are defined in the "Risk Accept" fields. In this sense, whenever the motivation of an attacker to harm the system was estimated to be low, due to a high cost burden relating to his malicious actions, no security controls were implemented, as we considered that the threat is unlikely to occur. In the same sense, whenever the implementation of a security control was too costly compared to the additional security benefits that it would add to the system we suggested that the enterprise should take the risk rather than invest in such a solution (e.g. the costs of biometric locks are too high to consider using such technology as a standard physical security control, so instead electronic keys were preferred).

The applicable legislations on data protection that differ across the world also affect the degree of applicability of our proposed security architecture for different enterprises. Since our legal requirements' focus was on European laws, it would be easier for enterprises residing in the European Union to tailor and utilize our proposed design for securing their mobility policies. Nevertheless, looking into US regulations, a different approach should be used in this case, due to the fact that US managers are given the freedom to access any type of information on devices used for business purposes, without the need for employee consent beforehand. What is more, the enterprise plans on integrating SaaS cloud applications could also be affected by such regulations, since vendors offering cloud space that spreads to locations outside the European Union should be approached differently to ensure compliance with the European GDPR, when formulating the enterprise service level agreements (SLAs). Finally, it has to be pointed out that the applicability of our proposed security architecture also depends on the type and size of the company. In this sense, a small-medium enterprise could still consider the financial burden related to the implementation of all proposed security components unacceptable, and thus its different approach would involve a higher rate of accepted residual risk.

6.4 Future research

Whereas our proposed artifact focuses on the implementation of an MDM system, in order to manage how data residing on the employee-owned devices is encrypted, which applications can be installed and what Smartphone features are permitted, new approaches on Smartphone BYOD are bubbling up from mobile hardware and software vendors.

One future security approach on Smartphone BYOD is mobile virtualization, which can unlock new opportunities and innovations to address business needs, by turning cloud-computing technology into an ally. Mobile virtualization enables the splitting of one Smartphone into two devices, by creating two instances of the same OS on the device. With this technology baked into future mobile devices, employees can have their personal and business information all in one Smartphone that is able to maintain independently operating identities. Dual-personality smart phones can provide true

isolation between the enterprise and personal interfaces, since employees see a completely different set of screens when they use the device for business access and when they use their Smartphone for personal purposes.

Effective virtualization can provide the balance between device security and usability. This multiple-identity Smartphone approach will be beneficial for the enterprise, as it protects mobility, collaboration and social computing. What is more, this solution will provide ease-of-use for employees, as they will be able to purchase a hypervisor-enabled Smartphone, according to their individual needs, and then let the enterprise activate the corporate policy on the device. At the same time, personal data privacy for the employees will be guaranteed, as the personal interface of the device will not be able to be seen or wiped by the corporate IT.

Mobile virtualization does not cancel out the currently proposed security architecture; rather it can seamlessly be integrated to an MDM system, through which the management of the corporate instance on the device will take place. However by starting with mobile devices based on virtual software partitions, MDM software can extend its capabilities for device management to enterprise-ready devices. In this sense, the IT administrators will be able customize the corporate image on the Smartphone with whatever applications the enterprise has chosen for its employees, while it could be remotely wiped if the phone is lost or stolen or if the employee leaves the company. Like today's enterprise approach, complementing network security controls should still be in place, such as the implementation of a VPN to limit the access on the corporate environment.

Consequently, an automated virtualization approach could enable the widespread adoption of Smartphone BYOD policies. Many enterprise IT departments are already looking at virtualization as a possible solution to the mobile BYOD security problem, that relates to simultaneously combating malware and hacking threats and still allowing employees the full range of functionality they prefer on their personal devices.

In a similar sense, further ideas have been suggested that go beyond the splitting of the Smartphone platform in order to cover potential security gaps. For example, there are suggested technologies related to employee prevention from using a Smartphone camera to take pictures of a company's intellectual property, which will be based on geo-fencing technology. In more detail, this technology implies that the camera and other relative Smartphone hardware or software features can be disabled when an employee is located in a certain area (e.g. a the manufacturing plant or the company campus), through the exploitation of the GPS tracking unit on the device.

On the downside, the suggested technological approaches on securing Smartphone BYOD will not be compatible with all mobile devices available in the market, due to additional processor and other hardware requirements. This means that the "anywhere, anytime" concept of mobility policies would be restrained, since employees will be required to choose from a limited device list. This restriction raises additional concerns

for the mobile employees, especially when enterprises require in their mobility policies that employees should cover all financial expenses related to the purchasing of Smartphone devices.

In the end, platform weaknesses will still be present on a split personality Smartphone, which employees could exploit to circumvent the personal and business platforms of their device and consequently capture business data on the personal side of their Smartphone. Nevertheless, this constitutes an HR rather than an IT management issue, since it is in the human nature that employees might always try to do something malicious. Such issues can only be resolved through employee awareness training and background checks, in order to reduce the insider threat as much as possible.

Bibliography

1. Subashini, S., and V. Kavitha. “A survey on security issues in service delivery models of cloud computing.” *Journal of Network and Computer Applications* 34.1 (2011): 1-11.

2. Walters, Richard. “The cloud challenge: ikipedia the benefits without increasing risk.” *Computer Fraud & Security* 2012.8 (2012): 5-12.

3. Copeland, Rebecca, and Noel Crespi. “Analyzing consumerization-Should enterprise business context determine session policy?.” *Intelligence in Next Generation Networks (ICIN), 2012 16th International Conference on*. IEEE, 2012.

4. Miller, Keith W., Jeffrey Voas, and George F. Hurlburt. “BYOD: Security and Privacy Considerations.” *IT Professional* 14.5 (2012): 53-55.

5. Dillon, Tharam, Chen Wu, and Elizabeth Chang. “Cloud computing: Issues and challenges.” *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*. IEEE, 2010.

6. Choo, Kim-Kwang Raymond. “Cloud computing: challenges and future directions.” *Trends and Issues in Crime and Criminal Justice* 400 (2010): 1-6.

7. Sultan, Nabil Ahmed. “Reaching for the “cloud”: How SMEs can manage.” *International journal of information management* 31.3 (2011): 272-278.

8. Bezemer, Cor-Paul, and Andy Zaidman. “Multi-tenant SaaS applications: maintenance dream or nightmare?.” *Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE)*. ACM, 2010.

9. Takabi, Hassan, James BD Joshi, and Gail-Joon Ahn. “Security and privacy challenges in cloud computing environments.” *Security & Privacy, IEEE* 8.6 (2010): 24-31.

10. Potts, Mike. “The state of information security.” *Network Security* 2012.7 (2012): 9-11.

11. Mansfield-Devine, Steve. “Interview: BYOD and the enterprise network.” *Computer Fraud & Security* 2012.4 (2012): 14-17.

12. Hevner, Alan R., et al. “Design science in information systems research.” *MIS quarterly* 28.1 (2004): 75-105.

13. Crook, Robert, et al. "Security requirements engineering: When anti-requirements hit the fan." *Requirements Engineering, 2002. Proceedings. IEEE Joint International Conference on*. IEEE, 2002.

14. Dhillon, Gurpreet, and James Backhouse. "Technical opinion: Information system security management in the new millennium." *Communications of the ACM* 43.7 (2000): 125-128.

15. Hanseth, Ole, and Kalle Lyytinen. “Theorizing about the design of Information Infrastructures: design kernel theories and principles.” (2004).

16. Spagnoletti, Paolo, Richard Baskerville, and Marco De Marco. "The contributions of Alessandro D’Atri to organization and information systems studies." *Designing Organizational Systems*. Springer Berlin Heidelberg, 2013. 1-18.

17. Furnell, Steven. “Securing mobile devices: technology and attitude.” *Network Security* 2006.8 (2006): 9-13.

18. Morrow, Bill. “BYOD security challenges: control and protect your most sensitive data.” *Network Security* 2012.12 (2012): 5-8.

19. Sabahi, Farzad. “Cloud computing security threats and responses.” *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*. IEEE, 2011.

20. Miller, Charlie. “Mobile attacks and defense.” *Security & Privacy, IEEE* 9.4 (2011): 68-70.

21. Kodeswaran, Palanivel, et al. “Securing Enterprise Data on Smartphones Using Run Time Information Flow Control.” *Mobile Data Management (MDM), 2012 IEEE 13th International Conference on*. IEEE, 2012.

22. Li, Xun, et al. “Smartphone Evolution and Reuse: Establishing a more Sustainable Model.” *Parallel Processing Workshops (ICPPW), 2010 39th International Conference on*. IEEE, 2010.

23. Portokalidis, Georgios, et al. “Paranoid android: versatile protection for smartphones.” *Proceedings of the 26th Annual Computer Security Applications Conference*. 2010.

24. Leavitt, Neal. “Mobile phones: the next frontier for hackers?.” *Computer* 38.4 (2005): 20-23.

25. Lawton, George. “Is it finally time to worry about mobile malware?.” *Computer* 41.5 (2008): 12-14.

26. Liu, Feng, et al. “SaaS integration for software cloud.” *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*. IEEE, 2010.

27. Tang, Yang, et al. “Fade: Secure overlay cloud storage with file assured deletion.” *Security and Privacy in Communication Networks*. Springer Berlin Heidelberg, 2010. 380-397.

28. Ugus, Osman, et al. “A Smartphone Security Architecture for App Verification and Process Authentication.” *Computer Communications and Networks (ICCCN), 2012 21st International Conference on*. IEEE, 2012.

29. Hofmann, Paul, and Dan Woods. “Cloud computing: the limits of public clouds for business applications.” *Internet Computing, IEEE* 14.6 (2010): 90-93.

30. Lonea, Alina Mădălina, Huaglory Tianfield, and Daniela Elena Popescu. "Identity management for cloud computing." *New Concepts and Applications in Soft Computing*. Springer Berlin Heidelberg, 2013. 175-199.

31. Sun, Wei, et al. "Software as a service: An integration perspective." *Service-oriented computing–ICSOC 2007*. Springer Berlin Heidelberg, 2007. 558-569.

32. Bekele, T. M., and Weihua Zhu. "Towards collaborative business process management development current and future approaches." *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*. IEEE, 2011.

33. Petcu, Dana, and Vlado Stankovski. "Towards Cloud-enabled Business Process Management Based on Patterns, Rules and Multiple Models." *Parallel and Distributed Processing with Applications (ISPA), 2012 IEEE 10th International Symposium on*. IEEE, 2012.

34. Scarfo, Antonio. "New Security Perspectives around BYOD." *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on*. IEEE, 2012.

35. Kwon, Hyeokchan, and Sin-Hyo Kim. "Efficient Mobile Device Management Scheme Using Security Events from Wireless Intrusion Prevention System." *Ubiquitous Information Technologies and Applications*. Springer Netherlands, 2013. 815-822.

36. Walker-Brown, Andrew. "Managing VPNs in the mobile worker's world." *Network Security* 2013.1 (2013): 18-20.

37. Rhee, Keunwoo, Woongryul Jeon, and Dongho Won. "Security Requirements of a Mobile Device Management System." *International Journal of Security and Its Applications* 6 (2012): 353-358.

38. Ma, Gun Il, et al. "Smartphone Remote Lock and Data Wipe System Based on Message Authentication Codes." *Applied Mechanics and Materials* 145 (2012): 267-271.

39. Gopalakrishnan, Anu. "Cloud computing identity management." *SETLabs briefings* 7.7 (2009): 45-54.

40. Armando, Alessandro, et al. "Securing the "Bring Your Own Device" Policy." *Journal of Internet Services and Information Security (JISIS)* 2.3/4: 3-17.

41. Hu, Bo, et al. "A Cloud Oriented Account Service Mechanism for SME SaaS Ecosystem." *Services Computing (SCC), 2012 IEEE Ninth International Conference on*. IEEE, 2012.

42. Park, Kyungwhan, et al. "Smartphone remote lock and wipe system with integrity checking of SMS notification." *Consumer Electronics (ICCE), 2011 IEEE International Conference on*. IEEE, 2011.

43. Almulla, Sameera Abdulrahman, and Chan Yeob Yeun. “Cloud computing security management.” *Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference on*. IEEE, 2010.

44. Costello, Tom, and Beverly Prohaska. “2013 Trends and Strategies.” *IT Professional* 15.1 (2013): 64-64.

45. Dinh, Hoang T., et al. “A survey of mobile cloud computing: architecture, applications, and approaches.” *Wireless Communications and Mobile Computing* (2011).

46. Nishikawa, K.; Oki, K.; Matsuo, A., “SaaS Application Framework Using Information Gateway Enabling Cloud Service with Data Confidentiality,” *Software Engineering Conference (APSEC), 2012 19th Asia-Pacific* , vol.1, no., pp.334,337, 4-7 Dec. 2012.

47. Absalom, Richard. "International Data Privacy Legislation Review: A Guide for BYOD Policies." (2012).

48. Josang, Audun, et al. “Security usability principles for vulnerability analysis and risk assessment.” *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*. IEEE, 2007.

49. Wahlgren, Gunnar, Khalid Bencherifa, and Stewart Kowalski. “A Framework for selecting IT Security Risk Management Methods based on ISO27005.”

50. Alberts, Christopher, et al. “Introduction to the OCTAVE Approach.” *Pittsburgh, PA, Carnegie Mellon University* (2003).

51. The Security Risk Management Guide, Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence. 2006.

52. Dobson, Ian, and Jim Hietala, eds. *Risk Management: The Open Group Guide*. Van Haren Pub, 2011.

53. Standard, I. S. O. "ISO 27005—Security Techniques—Information Security Risk Management." (2005).

54. Article 29 Data Protection Working Party. “Opinion 03/2013 on purpose limitation” 2013.

55. Article 29 Data Protection Working Party. “Opinion 02/2013 on apps on smart devices” 2013.

56. Information Commissioner’s Office (ICO). “Guidance on Bring Your Own Device” 2013.

57. Stoneburner, Gary, Clark Hayden, and Alexis Feringa. *Engineering principles for information technology security (a baseline for achieving security)*. BOOZ-ALLEN AND HAMILTON INC MCLEAN VA, 2001.

58. IBM_02, I. B. M. "Enterprise Security Architecture using IBM Tivoli Security Solutions; April 2002."

59. Stoneburner, Gary, Alice Goguen, and Alexis Feringa. "Risk management guide for information technology systems." *Nist special publication* 800.30 (2002): 800-30.

60. Bowen, Pauline, Joan Hash, and Mark Wilson. "SP 800-100. SP 800-100. Information Security Handbook: A Guide for Managers." (2006).

61. United States. Joint Task Force Transformation Initiative. *Recommended security controls for federal information systems and organizations*. US Department of Commerce, National Institute of Standards and Technology, 2009.

62. Grance, Timothy, Marc Stevens, and Marissa Myers. "Guide to selecting information technology security products." *Network Security* (2003).

63. PUB, FIPS. "Standards for Security Categorization of Federal Information and Information Systems." (2004).

64. Sherwood, John. "Clark; Andrew; Lynas, David."Systems and Business Security Architecture." SABSA Limited, 17 September 2003."

65. Oda, S. Michelle, Huirong Fu, and Ye Zhu. "Enterprise information security architecture a review of frameworks, methodology, and case studies." *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*. IEEE, 2009.

66. Brenner, Joel. "ISO 27001: Risk management and compliance." *RISK MANAGEMENT-NEW YORK*- 54.1 (2007): 24.

Appendix A – Detailed Assets List

Asset Name	High Level Description	Impact Class Rating
Data centers	Physical infrastructure	HBI
Servers	Physical infrastructure	HBI
Desktop/mobile computers	Physical infrastructure	LBI
Employee smart phones	Physical infrastructure	LBI
Routers	Physical infrastructure	MBI
Network switches	Physical infrastructure	MBI
Fax machines	Physical infrastructure	LBI
Removable media (portable hard drives, USB storage devices etc.)	Physical infrastructure	LBI
Power supplies	Physical infrastructure	MBI
Fire suppression systems	Physical infrastructure	MBI
Air filtration systems	Physical infrastructure	MBI
Telephony	Internal IT Services	MBI
File sharing	Internal/SaaS IT Services	HBI
E-mail/scheduling services	Internal/SaaS IT Services	HBI
Employee collaboration services (e.g. Microsoft Sharepoint)	Internal/SaaS IT Services	HBI
CRM services	Internal/SaaS IT Services	HBI
Mobile business application clients	Smartphone Service clients	MBI
Human resources data	Intranet/Extranet data	HBI
Financial data	Intranet/Extranet data	HBI
Marketing/product documentation data	Intranet/Extranet data	HBI
Employee credentials	Intranet/Extranet data	HBI
Employee business contact data	Intranet/Extranet data	MBI
Intellectual property	Intranet/Extranet data	HBI
Strategic plans	Intranet/Extranet data	HBI
Training materials	Intranet/Extranet data	MBI
Customer credit card data	Intranet/Extranet data	HBI
Customer contact data	Intranet/Extranet data	MBI
Customer medical records	Intranet/Extranet data	HBI
Customer purchase order data	Intranet/Extranet data	HBI
Supplier contract data	Intranet/Extranet data	HBI
Supplier contact data	Intranet/Extranet data	MBI

Supplier financial/purchase order data	Intranet/Extranet data	HBI
Cloud partner contract, financial and contact data	Intranet data	HBI
Business emails/ documents/contacts on enterprise workstations	Intranet data	MBI
Business emails/ documents/contacts on employee smart phones	Smartphone data	MBI
Employee personal data	Smartphone data	LBI
Reputation	Intangible	HBI
Goodwill	Intangible	MBI
Employee moral	Intangible	MBI
Employee productivity	Intangible	MBI

Table 8 – Detailed assets list. Adapted from (51)

Note: An Intranet/Extranet indication means that the storage location of the specific data depends on each enterprise's strategy of either storing them on the internal databases (Intranet) or on the enterprise cloud databases (Extranet). For each Internal/SaaS IT Service a corresponding mobile app is installed on the Smartphone device. Some customer and supplier data types only apply to enterprises in specific business domains.

Appendix B – Potential Threats

Threat	Example
High level description of the threat	*Specific example*
Catastrophic incident	Fire
Catastrophic incident	Flood
Catastrophic incident	Earthquake
Catastrophic incident	Severe storm
Catastrophic incident	Terrorist attack
Catastrophic incident	Civil unrest/riots
Catastrophic incident	Landslide
Catastrophic incident	Avalanche
Catastrophic incident	Industrial accident
Mechanical failure	Power outage
Mechanical failure	Hardware failure
Mechanical failure	Network outage
Mechanical failure	Environmental controls failure
Mechanical failure	Construction accident
Non-malicious person	Uninformed employee
Non-malicious person	Uninformed user
Malicious person	Hacker, cracker
Malicious person	Computer criminal
Malicious person	Industrial espionage
Malicious person	Government sponsored espionage
Malicious person	Social engineering
Malicious person	Disgruntled current employee
Malicious person	Disgruntled former employee
Malicious person	Terrorist
Malicious person	Negligent employee
Malicious person	Dishonest employee (bribed or victim of blackmail)
Malicious person	Malicious mobile code

Table 9 - Tailored potential threats list. Adapted from (51)

Appendix C – System Vulnerabilities

Vulnerability Class	Vulnerability	Example
High level vulnerability class	*Brief description of the vulnerability*	*Specific example (if applicable)*
Physical	Unguarded access to computing facilities	
Physical	Insufficient fire suppression systems	
Physical	Poorly constructed buildings	
Physical	Walls susceptible to physical assault	
Natural	Facility located on a fault line	
Hardware	Missing patches	
Hardware	Outdated firmware	
Hardware	Misconfigured systems	
Hardware	Systems not physically secured	
Hardware	Management protocols allowed over public interfaces	
Software	Out of date antivirus software	
Software	Missing patches	
Software	Deliberately placed weaknesses	Vendor backdoors for management or system recovery
Software	Deliberately placed weaknesses	Spyware such as keyloggers
Software	Deliberately placed weaknesses	Trojan horses
Software	Configuration errors	Manual provisioning leading to inconsistent configurations
Software	Configuration errors	Systems not audited
Communications	Unencrypted network protocols	
Communications	Unnecessary protocols allowed	
Communications	No filtering between network segments	
Human	Poorly defined procedures	Insufficient incident response preparedness
Human	Poorly defined procedures	Insufficient disaster recovery plans
Human	Poorly defined procedures	Testing on production systems
Human	Poorly defined procedures	Violations not reported
Human	Stolen credentials	

Table 10 - Tailored system vulnerabilities list. Adapted from (51)

Appendix D – Assessing Risk Stage Output

Key Information Risks										
	Asset		Exposure							
Risk ID	**Asset Name**	**Impact Class Rating**	**Defense-in-Depth Layer**	**Threat Description**	**Vulnerability Description**	**Exposure Rating (H,M,L)**	**Impact Rating (H,M,L)**	**Current Controls Description**	**Probability Rating w/Control (H,M,L)**	**Risk Rating w/Control (H,M,L)**
1.1	Internal/ enterprise cloud databases	HBI	Host	Disclosure/replication of corporate data through deliberately placed weaknesses on the Smartphone platform	Negligent employee deliberately overriding the enterprise security policies (e.g. via use of a jailbroken Smartphone, downloading applications from an untrusted app store)	M	M	Employee training on Smartphone BYOD policies including device protection best practices Background checks on employees	M	M
1.2	Internal/ enterprise cloud databases	HBI	Data	Low-level employees accessing restricted corporate data	Authentication mechanisms lack strong authorization rules for different employee positions	M	M	Single-factor authentication using username-password pairs Basic authorization mechanism (preventing lower level employees to access highly confidential information) Background checks on employees	M	M

1.3	Internal/ enterprise cloud databases	HBI	Host	Unauthorized access to corporate data through theft of employee credentials	Theft of credentials off managed **remote client** due to lack of antivirus software or outdated security patches on the Smartphone device	H	H	Employee training on Smartphone BYOD policies including device protection best practices	H	H
1.4	Internal/ enterprise cloud databases	HBI	Data	Unauthorized access to corporate data through theft of employee credentials	Theft of credentials via non technical means (e.g. eavesdropping, Social Engineering attacks)	H	H	Background checks on employees	L	M
1.5	Internal/ enterprise cloud databases	HBI	Data	Unauthorized access to corporate data by former employees	Former employee credentials are still active	H	H	Regular management of employee credentials including checks for inactive accounts	L	M
1.6	Internal/ enterprise cloud databases	HBI	Data	Disclosure of confidential data by a malicious current employee	Dishonest/ disgruntled current employees deliberately violating the confidentiality of data available to them	H	H	Background checks on employees Basic authorization mechanism (preventing lower level employees to access highly confidential information)	L	M

1.7	Internal/ enterprise cloud databases	HBI	Network	Unauthorized access to local corporate data by a malicious person (e.g. via Back Door software, IP Spoofing)	Weak perimeter defense and data encryption mechanisms, lack of sufficient audit tools and host configuration	H	H	Password protection on the enterprise Wi-Fi network Intranet firewalls for monitoring incoming/ outgoing traffic Data at rest is encrypted via a standard encryption algorithm	H	H
2.1	Internal corporate databases	HBI	Network	Disclosure/ modification of corporate data in transit by a malicious person (e.g. Sniffing attacks, Man-in-the Middle attacks)	Weak perimeter/ network protection mechanisms	H	H	Password protection on the enterprise Wi-Fi network Intranet firewalls for monitoring incoming/ outgoing traffic	H	H
2.2	Internal corporate databases	HBI	Application	Unauthorized access to the internal applications by a malicious person through Password attacks	Poor authentication mechanisms used for accessing the internal applications	H	H	Single-factor authentication using username-password pairs Employee training on protection/ regular updating of credentials	M	M
2.3	Internal corporate databases	HBI	Host	Unauthorized access to corporate data through theft of employee credentials	Theft of credentials off **local host** via outdated configuration of antivirus signatures, host configuration, or outdated security patches on the enterprise servers	H	H	Antivirus software installed on local servers/ workstations Intranet firewalls for monitoring incoming/ outgoing traffic Regular checks on available system updates and patches for the local hardware	H	H

3.1	External corporate databases on the Cloud	HBI	Application	Unauthorized access to the enterprise SaaS applications by a malicious person through Password attacks	Poor authentication mechanisms used for accessing the SaaS applications	H	H	Reliance on the cloud vendor's authentication mechanisms	M	M
3.2	External corporate databases on the Cloud	HBI	Network	Unauthorized access to corporate data on the enterprise cloud by a malicious person	Insufficient defense and data encryption mechanisms on the cloud	H	H	Reliance on cloud vendor for host/ data security mechanisms	M	M
4.1	Data centers/ Servers	HBI	Physical	Damage by a catastrophic incident (e.g. fire, flood)	Poorly designed/ constructed buildings	H	H	Standard security mechanisms for buildings (door locks, security guards etc) Fire alarms/ Smoke detectors	L	L
4.2	Data centers/ Servers	HBI	Physical	Damage/ Theft of hardware by a malicious person	Lack of sufficient physical security measures in the enterprise	H	H	Standard security mechanisms for buildings (door locks, security guards etc)	L	M
4.3	Data centers/ Servers	HBI	Host	Interruption of business services due to flooding attacks on the enterprise servers	Lack of sufficient server security measures against High Load/ Denial-of-Service attacks	H	H	Standard backup/ recovery mechanisms Intranet firewalls for monitoring/ blocking heavy incoming traffic	H	H
5.1	Enterprise workstations	LBI	Physical	Damage by a catastrophic incident/ mechanical failure	Poorly designed/ constructed buildings Faulty hardware unit	H	L	Standard security mechanisms for buildings (door locks, security guards etc) Fire alarms/ Smoke detectors	L	L

5.2	Enterprise workstations	LBI	Physical	Damage/ Theft of hardware by a malicious person	Lack of sufficient physical security measures in the enterprise	H	L	Standard security mechanisms for buildings (door locks, security guards etc)	L	L
6.1	Corporate data on enterprise workstations	MBI	Host	Unauthorized access to corporate data through the employee workstation	Uninformed/ negligent employee leaving his workstation unattended while logged on the enterprise services	M	M	No controls	M	M
7.1	Power supplies/ Telephony lines	MBI	Physical	Damage by a catastrophic incident (e.g. fire, flood)	Poorly designed/ constructed buildings	H	M	Standard security mechanisms for buildings (door locks, security guards etc) Fire alarms/ Smoke detectors	L	L
7.2	Power supplies/ Telephony lines	MBI	Physical	Damage by a malicious person	Lack of sufficient physical security measures in the enterprise	H	M	Standard security mechanisms for buildings (door locks, security guards etc)	L	L
8.1	Employee smart phones	LBI	Physical	Loss/ Theft of personal device	Negligent employee leaving a device unattended	M	L	No controls	M	L

9.1	Corporate data on employee smart phones	MBI	Data	Unauthorized access to corporate data stored on the device by a malicious person	Lack of security measures for cases of a device being lost/ stolen	M	M	No controls	M	M
9.2	Corporate data on employee smart phones	MBI	Data	Unauthorized access to corporate data stored on the device by former employees	Confidential data still present locally on employee devices after leaving the enterprise	H	M	No controls	M	M
9.3	Corporate data on employee smart phones	MBI	Data	Unauthorized access to corporate data stored on the device by family members	Uninformed/ negligent employee leaving his Smartphone unattended/delibe rately sharing the device with other family members	M	M	Employee training on Smartphone BYOD policies including device protection best practices	L	L
9.4	Corporate data on employee smart phones	MBI	Data	Unauthorized access to corporate data stored on the device by the device manufacturer	Lack of security policies for cases of a device being sent for replacement/ service to the manufacturer	M	M	No controls	L	L
10.1	Employee personal data	LBI	Data	Legal prosecution against the enterprise for violating employee privacy rights during Smartphone monitoring	Lack of appropriate legislation related to the protection of employee privacy	L	L	No controls	H	M

Table 11 - Assessing risk stage output

Appendix E – Decision Support Stage Output

Risk ID	Action (Avoid, Control, Accept, Transfer)	Relative Control Sets
1.1	Mitigate	1. Deploy a Mobile Device Management system to enroll/manage the smart phone devices that are allowed to access the corporate network/data. Blacklist devices that are jailbroken/routed since they can be easily compromised. 2. Work with the security and business team to establish acceptable-use policies regarding allowed protocols, services and features for the corporate hardware and the employee Smartphone devices. Document the policies and make them available on the corporate intranet. Also consider introducing them as part of new employee orientation. 3. Monitor the employee devices to ensure that their configuration is in line with corporate restrictions on the installation of specific apps and on the disabling of specific software/sensor features.
1.2	Mitigate	1. Applications should implement an authorization mechanism that provides access to sensitive data and functionality only to suitably permitted users or clients. 2. Role-based access controls should be enforced at database level as well as at the application interface. This will protect the database in the event that the client application is exploited. 3. Enable logging across all applications in the environment, in order to monitor failed and successful authentication attempts and changes to application data. 4. Authorization checks should require prior successful authentication to have occurred. 5. Perform regular background checks for all employees, regardless of position to identify any potential issues that could put at risk the organization and/or other employees.
1.3	Mitigate	1. Deploy a Mobile Device Management system to enroll/manage the smart phone devices that are allowed to access the corporate network/data. Blacklist devices that are jailbroken/routed since they can be easily compromised. 2. Install and actively manage anti-virus/anti-malware clients on the smart phones from the centralized MDM server for configuration and signature deployment.

		3. The remote clients on the employee smart phones should automatically check in with the enterprise MDM server upon successful authentication, through which critical software updates/patches will be pushed to the devices. 4. Work with the security and business team to establish acceptable-use policies regarding allowed protocols, services and features for the corporate hardware and the employee Smartphone devices. Document the policies and make them available on the corporate intranet. Also consider introducing them as part of new employee orientation. 5. Monitor the employee devices to ensure that their configuration is in line with corporate restrictions on the installation of specific apps and on the disabling of specific software/sensor features.
1.4	Mitigate	1. Deploy multifactor authentication for both internal and remote users connecting over the Internet to corporate resources. 2. Lifetime and pre-expiration of passwords should all be set to provide additional defenses. 3. Enable logging across all applications in the environment, in order to monitor failed and successful authentication attempts and changes to application data. 4. Provide security awareness training for all employees on a quarterly basis and cover all aspects of security, including security policies and controls, reporting suspicious activity, privacy, e-mail security, Internet security, and computer security. Security awareness should be mandatory as part of new employee orientation. 5. Perform regular background checks for all employees, regardless of position to identify any potential issues that could put at risk the organization and/or other employees.
1.5	Mitigate	1. Initiate an immediate notification procedure to all system administrators for terminated staff members to ensure their accounts are disabled immediately, especially their remote access accounts. 2. Conduct regular reviews on the current accounts of staff that transfer to another department within the organization. 3. Develop with the HR department a formal employee exit policy including separate policies for friendly and hostile terminations. 4. Lifetime and pre-expiration of passwords should all be set to provide additional defenses.
1.6	Mitigate	1. Perform regular background checks for all employees, regardless of position to identify any potential issues that could put at risk the organization and/or other employees. 2. Develop with the HR department a formal employee exit policy including separate policies for friendly and hostile terminations. 3. Enable logging across all applications in the environment, in order to monitor failed and successful authentication attempts and changes to application data.

1.7	Mitigate	1. Deploy VPN for remote-user-access connectivity. 2. Implement packet filtering via router ACLs (Access Control Lists). 3. Install host-based firewall software and implement highly restrictive firewall rules. The firewalls should be in place with a default deny stance, allowing only traffic that is necessary. 4. Deploy either host- or network-based intrusion-detection systems. 5. Encrypt all confidential corporate data at rest using strong algorithms.
2.1	Mitigate	1. Deploy VPN for remote-user-access connectivity. 2. The implementation of the enterprise Wi-Fi network should include non-broadcast of SSID, WPA encryption and treating the network as untrusted. 3. Deploy firewalls and frequently test and verify that they are working properly. 4. Deploy network-based intrusion-detection systems.
2.2	Mitigate	1. Implement an authentication mechanism based on a single sign-on paradigm that allows mobile employees to access the corporate resources without performing dedicated log in for each separate application. 2. Deploy multifactor authentication for both internal and remote users connecting over the Internet to corporate resources. For the case of remote access via employee smart phones regularly audit the access list for all the users on the VPN device. 3. Implement an authentication mechanism with complex passwords of 8 to 14 characters in length, with alphanumeric and special characters. Minimum length, history maintenance, lifetime, and pre-expiration of passwords should all be set to provide additional defenses. 4. Implement thresholds on failed authentications so that alerts can be sent to systems administrators and perform regular tests on the password policies in place.
2.3	Mitigate	1. Deploy a DMZ segment as part of a systematic and formal firewall development, in order to protect the remote access of internal corporate resources. 2. Install host-based firewall software and implement highly restrictive firewall rules. The firewalls should be in place with a default deny stance, allowing only traffic that is necessary. 3. Deploy anti-virus solutions throughout the environment on both the server and workstation levels. Configure anti-virus solutions to scan for viruses both entering and leaving the environment. Extend anti-virus solutions to mail, database and web servers through file server scanners, content screening tools and data upload and download scanners. 4. Deploy either host- or network-based intrusion-detection systems.

3.1	Transfer/Mitigate	1. Implement an authentication mechanism based on a single sign-on paradigm for the SaaS services using the employee credentials that are stored in the enterprise's active directory. The mechanism should be based on a trust relationship between the enterprise MDM server and a corresponding federation server located on the SaaS provider's network. 2. Deploy multifactor authentication for both internal and remote users connecting over the Internet to corporate resources. For the case of remote access via employee smart phones regularly audit the access list for all the users on the VPN device. 3. Implement an authentication mechanism with complex passwords of 8 to 14 characters in length, with alphanumeric and special characters. Minimum length, history maintenance, lifetime, and pre-expiration of passwords should all be set to provide additional defenses. 4. Implement thresholds on failed authentications so that alerts can be sent to systems administrators and perform regular tests on the password policies in place.
3.2	Transfer/Mitigate	1. In order to securely process data via SaaS applications, dynamically switch the executing environment to the enterprise environment by using a deploying sandbox. Route only secured/encrypted data to the cloud environment. 2. Encrypt all confidential corporate data at rest using strong algorithms. 3. Formulate a cloud service security policy to define the cloud provider privileges and the physical location of corporate data stored on the cloud environment. Include procedures that ensure deletion of all data remanence from the cloud.
4.1	Mitigate/Accept	1. Secure the enterprise facilities via physical controls (electronic locks, perimeter fencing, security guards) and alarm systems. Frequently test the system (in conjunction with the alarm company) to ensure that it is working properly.
4.2	Mitigate	1. Migrate network equipment/servers in lockable cabinets/racks in order to protect against unauthorized tampering. 2. Initiate physical access controls (such as employee and visitor badges, visitor escorts, visitor logs) to guard against unauthorized people gaining access to the building and to sensitive information. 3. Increase staff awareness of the personnel access control policy and encourage the challenging of unrecognized individuals.
4.3	Mitigate	1. Deploy clustering mechanisms to ensure high availability for critical databases and file shares. 2. Deploy hardware load balancers to achieve higher availability. 3. Implement packet filtering via router ACLs (Access Control Lists). 4. Install host-based firewall software and implement highly restrictive firewall rules. The firewalls should be in place with a default deny stance, allowing only traffic that is necessary. 5. Deploy network-based intrusion-detection systems.

		6. Formulate up-to-date disaster recovery and business continuity plans that relate to the recovery from catastrophic evens that affect a large fraction of the firm's IT infrastructure. The planning should cover the entire technological, physical and staff environment and should be regularly tested to validate correctness and completeness.
5.1	Mitigate/Accept	1. Secure the enterprise facilities via physical controls (electronic locks, perimeter fencing, security guards) and alarm systems. Frequently test the system (in conjunction with the alarm company) to ensure that it is working properly.
5.2	Mitigate	1. Secure workstations/laptops with cable locks, in order to prevent theft. 2. Encrypt all confidential corporate data at rest using strong algorithms. 3. Initiate physical access controls (such as employee and visitor badges, visitor escorts, visitor logs) to guard against unauthorized people gaining access to the building and to sensitive information. 4. Increase staff awareness of the personnel access control policy and encourage the challenging of unrecognized individuals.
6.1	Mitigate	1. All users should have a password-protected screen saver with a short time-out period. 2. Provide security awareness training for all employees on a quarterly basis and cover all aspects of security, including security policies and controls, reporting suspicious activity, privacy, e-mail security, Internet security, and computer security. Security awareness should be mandatory as part of new employee orientation.
7.1	Mitigate/Accept	1. Secure the enterprise facilities via physical controls (electronic locks, perimeter fencing, security guards) and alarm systems. Frequently test the system (in conjunction with the alarm company) to ensure that it is working properly.
7.2	Mitigate	1. Initiate physical access controls (such as employee and visitor badges, visitor escorts, visitor logs) to guard against unauthorized people gaining access to the building and to sensitive information. 2. Increase staff awareness of the personnel access control policy and encourage the challenging of unrecognized individuals.

8.1	Mitigate/Accept	1. Provide security awareness training to all employees as part of new employee orientation and on a quarterly basis. Cover aspects of personal device protection best practices.
9.1	Mitigate	1. Implement remote wipe/lock tools to avoid leakage of confidential corporate data. 2. Enforce a strong PIN policy for Smartphone devices. 3. Encrypt all confidential corporate data at rest using strong algorithms.
9.2	Mitigate	1. Implement remote wipe tools to avoid leakage of confidential corporate data. 2. Develop with the HR department a formal employee exit policy including separate policies for friendly and hostile terminations. 3. Define and implement formal procedures for the management and disposal of information in electronic form that is contained on external storage of employee smart phones and ensure that all users know the proper practices.
9.3	Mitigate	1. Enforce a strong PIN policy for Smartphone devices. 2. Avoid automatically authorizing devices based on identifiers like MAC address alone, so that guest users of a device must still present credentials to access sensitive data. 3. Provide security awareness training to all employees as part of new employee orientation and on a quarterly basis. Cover aspects of personal device protection best practices.
9.4	Mitigate	1. Implement remote wipe tools to avoid leakage of confidential corporate data. 2. Encrypt all confidential corporate data at rest using strong algorithms. 3. Define and implement formal procedures for the management and disposal of information in electronic form that is contained on external storage of employee smart phones and ensure that all users know the proper practices.
10.1	Mitigate	1. Implement a formal mobility policy that complies with the European legislations on data protection. 2. Third-party audits should be performed regularly to ensure compliance with all current legal requirements.

Table 12 - Decision support stage output

Appendix F – List of Proposed Security Controls

Area-of-Analysis	Functionality	Proposed Control
operational	preventive/ detection	Secure the enterprise facilities via physical controls (electronic locks, perimeter fencing, security guards) and alarm systems. Frequently test the system (in conjunction with the alarm company) to ensure that it is working properly.
operational	preventive/ detection	Initiate physical access controls (such as employee and visitor badges, visitor escorts, visitor logs) to guard against unauthorized people gaining access to the building and to sensitive information.
organizational	preventive	Increase staff awareness of the personnel access control policy and encourage the challenging of unrecognized individuals.
technical	preventive	Deploy VPN for remote-user-access connectivity.
technical	preventive	The implementation of the enterprise Wi-Fi network should include non-broadcast of SSID, WPA encryption and treating the network as untrusted.
technical	preventive	Deploy firewalls and frequently test and verify that they are working properly.
operational	preventive	Migrate network equipment/servers in lockable cabinets/racks in order to protect against unauthorized tampering.
technical	preventive	Deploy clustering mechanisms to ensure high availability for critical databases and file shares.
technical	preventive	Deploy hardware load balancers to achieve higher availability.
technical	preventive	Implement packet filtering via router ACLs (Access Control Lists).

technical	preventive	Install host-based firewall software and implement highly restrictive firewall rules. The firewalls should be in place with a default deny stance, allowing only traffic that is necessary.
organizational	recovery	Formulate up-to-date disaster recovery and business continuity plans that relate to the recovery from catastrophic evens that affect a large fraction of the firm's IT infrastructure. The planning should cover the entire technological, physical and staff environment and should be regularly tested to validate correctness and completeness.
operational	preventive	Secure workstations/laptops with cable locks, in order to prevent theft.
technical	preventive	Encrypt all confidential corporate data at rest using strong algorithms.
technical	preventive	All users should have a password-protected screen saver with a short time-out period.
organizational	preventive	Provide security awareness training for all employees on a quarterly basis and cover all aspects of security, including security policies and controls, reporting suspicious activity, privacy, e-mail security, Internet security, and computer security. Cover aspects of personal device protection best practices. Security awareness should be mandatory as part of new employee orientation.
technical	preventive	Implement remote wipe/lock tools to avoid leakage of confidential corporate data.
organizational	preventive	Enforce a strong PIN policy for Smartphone devices.
organizational/ operational	preventive	Define and implement formal procedures for the management and disposal of information in electronic form that is contained on external storage of employee smart phones and ensure that all users know the proper practices.
technical	preventive	Avoid automatically authorizing devices based on identifiers like MAC address alone, so that guest users of a device must still present credentials to access sensitive data.
technical	preventive	Implement an authentication mechanism based on a single sign-on paradigm that allows mobile employees to access the corporate resources without performing dedicated log in for each separate application.
technical	preventive	Deploy multifactor authentication for both internal and remote users connecting over the Internet to corporate resources. For the case of remote access via employee smart phones regularly audit the access list for all the users on the VPN device.

organizational/ technical	preventive/ recovery	Implement an authentication mechanism with complex passwords of 8 to 14 characters in length, with alphanumeric and special characters. Minimum length, history maintenance, lifetime, and pre-expiration of passwords should all be set to provide additional defenses.
technical	detection	Implement thresholds on failed authentications so that alerts can be sent to systems administrators and perform regular tests on the password policies in place.
technical	preventive	Implement an authentication mechanism based on a single sign-on paradigm for the SaaS services using the employee credentials that are stored in the enterprise's active directory. The mechanism should be based on a trust relationship between the enterprise MDM server and a corresponding federation server located on the SaaS provider's network.
organizational/ technical	preventive	Applications should implement an authorization mechanism that provides access to sensitive data and functionality only to suitably permitted users or clients.
organizational/ technical	preventive	Role-based access controls should be enforced at database level as well as at the application interface. This will protect the database in the event that the client application is exploited.
technical	detection	Enable logging across all applications in the environment, in order to monitor failed and successful authentication attempts and changes to application data.
technical	detection	Authorization checks should require prior successful authentication to have occurred.
organizational	preventive/ detection	Perform regular background checks for all employees, regardless of position to identify any potential issues that could put at risk the organization and/or other employees.
technical	preventive/ detection/ recovery	Deploy a Mobile Device Management system to enroll/manage the smart phone devices that are allowed to access the corporate network/data. Blacklist devices that are jailbroken/routed since they can be easily compromised.
technical	detection/ recovery	Install and actively manage anti-virus/anti-malware clients on the smart phones from the centralized MDM server for configuration and signature deployment.
technical	preventive/ recovery	The remote clients on the employee smart phones should automatically check in with the enterprise MDM server upon successful authentication, through which critical software updates/patches will be pushed to the devices.

organizational	preventive	Work with the security and business team to establish acceptable-use policies regarding allowed protocols, services and features for the corporate hardware and the employee Smartphone devices. Document the policies and make them available on the corporate intranet. Also consider introducing them as part of new employee orientation.
technical	detection	Monitor the employee devices to ensure that their configuration is in line with corporate restrictions on the installation of specific apps and on the disabling of specific software/sensor features.
organizational	recovery	Initiate an immediate notification procedure to all system administrators for terminated staff members to ensure their accounts are disabled immediately, especially their remote access accounts.
organizational	detection	Conduct regular reviews on the current accounts of staff that transfer to another department within the organization.
organizational	preventive	Develop with the HR department a formal employee exit policy including separate policies for friendly and hostile terminations.
technical	preventive	Deploy a DMZ segment as part of a systematic and formal firewall development, in order to protect the remote access of internal corporate resources.
technical	detection/ recovery	Deploy anti-virus solutions throughout the environment on both the server and workstation levels. Configure anti-virus solutions to scan for viruses both entering and leaving the environment. Extend anti-virus solutions to mail, database and web servers through file server scanners, content screening tools and data upload and download scanners.
technical	detection/ recovery	Deploy either host- or network-based intrusion-detection systems.
technical	preventive	In order to securely process data via SaaS applications, dynamically switch the executing environment to the enterprise environment by using a deploying sandbox. Route only secured/encrypted data to the cloud environment.
organizational	preventive	Formulate a cloud service security policy to define the cloud provider privileges and the physical location of corporate data stored on the cloud environment. Include procedures that ensure deletion of all data remanence from the cloud.
organizational	preventive	Implement a formal mobility policy that complies with the European legislations on data protection.
organizational	detection	Third-party audits should be performed regularly to ensure compliance with all current legal requirements.

Table 13 - Proposed security controls