Towards a Reference Architecture for Privacy Aware Health Care Organizations

---

Wouter Aker

July 13, 2018
Version: Final

Final Project

Master Business Information Technology

Towards a Reference Architecture for Privacy Aware Health Care Organizations

Wouter Aker
s0193852

First Supervisor Maria Iacob
Faculty of Behavioural Management and Social Sciences
University of Twente

Second Supervisor Marten van Sinderen
Faculty of Electrical Engineering, Mathematics and Computer Science
University of Twente

External Supervisor Marcel Tonnis
Information Manager
Welzorg Nederland B.V.

University of Twente
Enschede, The Netherlands

July 13, 2018

Executive Summary

With the introduction of the GDPR the subject privacy became a hot topic in almost every European organization. Some might say the collection and processing of personal information got the attention it deserved. Fact is that in Europe the collecting and processing of personal information is regulated by privacy laws.

Organizations in the health care industry also need to be compliant with these privacy rules and regulation, like every other organization. This can be more challenging for these organization in comparison to organizations in general due to the nature of their activities. These activities require them to process health care records with is seen as sensitive personal information.

Besides, these organization operate in a public or semi public environment. Many activities are financed by social health care laws. To prevent fraud these laws require health care organizations to collect some personal information, like an identification number.

All organizations in the health care industry deal with the same challenges. A reference architecture can be part of a solution. With the privacy risks and personal information management methodology organizations are able to identify vulnerabilities and getting control over the associated risks.

This detailed methodology has a step by step description of activities that together help organization to monitor business processes, identify vulnerabilities, threats and risks and select appropriate control measures. The application of the methodology at medical equipment supplier Welzorg shows the value of such a methodology.

Multiple vulnerabilities were identified including weak authorization and authentication processes, the use of papers containing personal information and a lack of privacy awareness. By selecting appropriate control measures based on ISO 27001 control objectives these vulnerabilities were mitigated. The implementation of a centralized authentication and authorization system and a continues privacy awareness program are examples of new projects that fulfill these control measures.

This methodology is only part of the solution and has its limitations. But with this methodology you can thoroughly analyze critical processes in health care organization to reduce the risk of violating privacy rules and regulations.

Contents

1 Introduction

1.1 Motivation

Every now and then there is news about a data leakage. Hacked information systems, stolen laptops or USB-sticks are often the source of these leakages. But almost as often the source is a due to human mistakes like poorly protected information systems, accidentally unauthorized access or wrongly configured systems. But often seen as the weakest link are the end user of the systems. Intentionally and unintentionally they provide unauthorized access to sensitive information.

Privacy and the security of personal information are topics that more and more people become aware of. Social media companies for example that collect and store massive amounts of personal data are critically looked at by data protection supervisors. Users increasingly are aware of the risks associated with the collection of personal information.

In many countries there are rules regulating the collection, processing and storage of personal data. In the European Union every country has laws based on a European Directive regarding the protection of their citizens' personal data. In The Netherlands this used to be the Data Protection Act (*Wet bescherming persoonsgegevens* (2000), WBP) and now is the Dutch implementation of the (*General Data Protection Regulation* 2016). These regulate the collection, processing and storage of personal data. These act gives the Dutch citizens the right to know why and how organizations use their personal data.

The processing of certain special categories of personal data is extra protected because of the sensitivity of the data. Personal data concerning someone's health and national identification numbers for example are considered as sensitive information and therefore protected by strict regulations. The processing of this data is only allowed when it is explicitly regulated.

Some organizations have to process data concerning the health of their client due to the nature of their activities. These organizations are allowed to process this data to be able to do their work. Hospitals, dentists, health insurance companies or even opticians all process, to the greater of to the lesser extent, personal data concerning the health of the customers and clients.

Another example are organizations delivering medical devices like wheelchairs, scooters, nursing beds and so on. These organizations need to some extinct collect and process medical data to be able to deliver the most suitable medical device.

Besides the personal data concerning health, there is a second set of data which is categorized as a special. The Dutch national identification number (Burgerservicenummer 2007, BSN) is a national identification number issued by the Dutch government. It is used for communication with many governmental organizations and even some semi-public or private organizations. However, the private organizations that use the BSN need to have a legal base to be allowed to process the BSN. This is the case for some private organizations operating in the health industry, like health insurers, and organization that interact with them, like the suppliers of medical devices.

With the collection of the personal data in these special categories come responsibilities. The personal data should be protected well and used only for the purpose it was collected for. Suppliers of medical devices too have to be compliant with rules and regulations regarding privacy. This can be challenging, especially when working in the health sector where you have to deal with many external stakeholders. Both the processes and the information technology used in these organizations have to be designed to comply with rules, regulations, industry standards and agreements with these stakeholders.

Welzorg (2017) is a supplier of medical supplies and equipment operating in the Netherlands and specialized in advisory, delivery, service and customization of health care products for medical needs at home. They deliver health care products like wheelchairs, scooters, crutches, shower seats and bedding, almost always lending the products short or long term. Welzorg is part of the Louwman Group, a large automotive distributor in Europe. Welzorg is a bit of a stranger in the midst since they fully focus on the health industry where other subsidiaries of Louwman focus on the automotive industry. Due to the nature of their activities Welzorg processes a lot of personal data, some of which is classified as special personal data. In order to comply to regulations regarding data security, to be able to satisfy customers' demands regarding privacy and to reassure clients their personal data is processes discreetly proper control mechanisms should be in place.

1.2 Background

Working in the health industry can be a complex matter. In the Netherlands different laws together form the national health care system. These are the Social Support Act (*Wet maatschappelijke ondersteuning 2015* (2014), WMO), the Long-term Care Act (*Wet langdurige zorg* (2014), WLZ) and the Heath Insurance Act (*Zorgverzekeringswet* (2005), ZVW). Depending on the kind of care someone needs, it is covered by one of these acts. The acts are executed by different

organizations. The WMO is executed by municipalities, the ZVW by health insurers and the WLZ by so called care offices (Dutch: Zorgkantoren). This means that organizations delivering health services covered by the health care system have to deal with the regulations of these acts and their executors.

In the Netherlands there are currently 344 municipalities. Each municipality is responsible for the execution of the WMO for their citizens. This means they have to contract companies who provide the services that are covered by this health act. Because the municipalities are public organizations they have to act according to European procurement rules and openly invite tenders to make an offer to deliver the required services. Every municipality can, within the borders of the procurement rules, write down their own requirements and focus on certain aspects which are important for their citizens. This results in a wide range of contract formats that is used in this industry.

On 4 May 2016 the European Union (EU) published her new *General Data Protection Regulation* (2016). These European regulations give citizen more right regarding the processing of their personal data and give organizations who process personal data more responsibilities. This act will be into force from 25 May 2018 on forward. This act replaced current data protection laws of the members of the European Union. There were two main reasons for the EU to write a new privacy regulation. First of all the raise of information technology. This adds new challenges to the protection of personal data. The new regulation takes into account these new challenges like big data processing and globally active social networks and should therefore be future proof. The second reason to publish the new regulation was to make the European market more equal so organizations can more easily operate in multiple countries. When the organization complies to the implementation of the European Data Protection Act in one country, it complies to the Data Protection Law in all European countries.

Summarizing, companies like Welzorg are active in a vibrant industry. They have to deal with challenges that come with the complex health care system, have to fulfill the requirements of all the different contracts and have to comply to increasingly strict privacy regulations. In order to be able to fulfill the requirements there has to be a good understanding of the industry organizations like Welzorg are active in. There has to be clear which privacy regulations are applicable and which have to be satisfied. Next, a general solution has to be chosen or designed with which organizations active in this industry can systematically make sure they comply to all the applicable regulations.

1.3 Objective

For many organizations it is already a challenge to implement controls in order to be compliant with the new privacy rules and regulations. For organizations operating in public health care

industry this can even be more challenging. Not only do they operate in a complex web of social laws financing the public health care, they also have to deal with sensitive data about someone's health. These organizations need a structured methodology to assess the current risks regarding the processing and collecting of personal information. This should help them to make suitable measures to mitigate risks and thereby comply with privacy rules and regulations.

Therefore, the goal of this research will be:

To develop an element of a reference architecture for organizations active in the health industry which is compliant with privacy regulations and thereby reduces the risks associated with no being compliant

1.4 Scope

The health care industry is a huge industry with many different types of organizations. This research will primarily focus on the main process of organizations in the medical supplies lending industry. The main process of these organizations can be related to the life cycle of a medical device delivery. On a high level this live cycle can be broken down into three steps. The first being the request handling and delivery of the device, the second being the maintenance of the device and the third being the return of the device (Fig. 1.1).

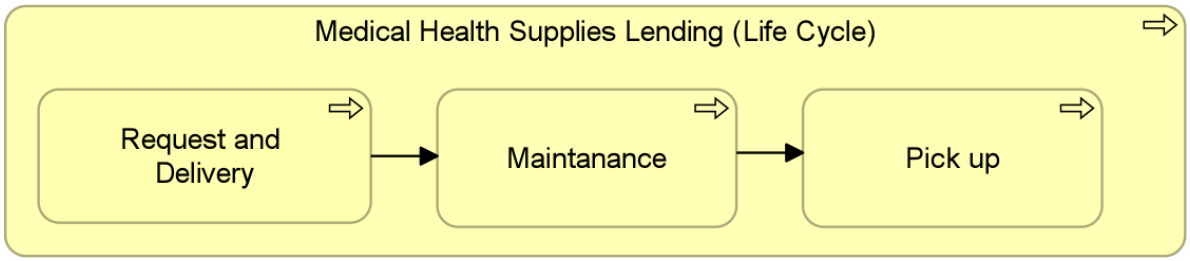

Fig. 1.1: Medical Health Supplies Lending Life Cycle

This research will focus on the personal information of the clients in need of a medical device. All other personal information that may or may not be collected and processed by the health care organizations will be out of scope. Personal information related to employees or other stakeholders for example.

Finally, only the four main delivery channels will be in scope. These main delivery channels are:

- WMO requests
- WLZ requests
- ZVW requests
- Direct sells (Online and stores)

This implicitly means this research will focus on the Dutch health care industry and therefore primarily focus on Dutch rules and regulations when applicable.

1.5 Research Questions

To be able to achieve the goal as stated earlier we have to answer some questions. These research questions help to understand the underlying problem and to give a direction towards a possible solution. The research questions are:

1. Which privacy regulation(s) do organizations in the health care industry have to comply to?

    a) How does the Dutch health care systems work?
    b) What are the current privacy rules and regulations in the Netherlands?
    c) What is the risk of not being compliant?
    d) How to organize regulatory compliance?

2. Can we define an element of a reference architecture to help organizations in the medical supplies lending industry to be compliant with privacy rules and regulations?

    a) What is a reference architecture?
    b) Which methodology or framework is suitable to define a reference architecture?
    c) What is an appropriate reference architecture for the medical supplies lending industry?

3. How does the defined element perform?

    a) How does the solution perform in practice?
    b) How is the the designed solution evaluated in theory?

During the research we will try to answer all questions above.

1.6 Research Methodology

The approach used for this research will be based on the methodology proposed by Peffers et al. (2007) and shown in (Fig. 1.2). This Design Science Research Methodology (DSRM) is developed for research in the IS domain and a commonly accepted framework for the development of artifacts. The methodology describes 6 activities: problem identification and motivation, define objectives of a solution, design and development, demonstration, evaluation,

and communication. Although according to DSRM one can start with any activity this research will start with the first activity and successively carry out the activities since the initiation of the research is problem-centered.

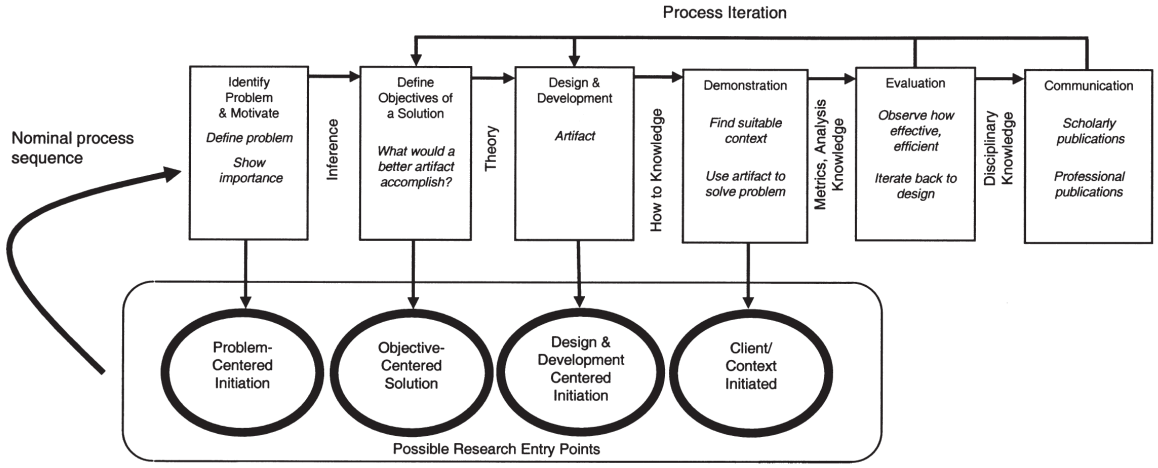

Fig. 1.2: Peffers et al. (2007) - Design Science Research Methodology Process Model

The research will start with the problem identification and motivation. During this phase the specific research problem will be defined and the importance of a solution will be shown. Interviews with the client and some research will make clear why the development of an artifact is needed. This will result in a clear motivation for this research, some background information and finally a research goal.

Next, the objectives for a solution are defined. Some literature research is needed to acquire knowledge that is needed to understand the problem and the context. Furthermore, the literature research will also focus on current solutions for similar problems. The literature research will focus on regulatory compliance, reference and enterprise architectures, risk and security, privacy rules and regulations and the Dutch health care system.

The actual design and development of the artifact is the fourth activity that is performed. This includes the description of the desired functionality and its architecture. The design of the artifact, a reference architecture, will be based on the findings previously carried out literature research.

The demonstration and evaluation activities will be executed together. The demonstration of the artifact shows how it is used to solve the previously defined research problem. The evaluation shows how well the artifact supports a solution for the problem.

The final activity is the communication. It is important to communicate the importance to solve the problem, the need for a solution, how the artifact contributes to the solution and its effectiveness.

1.7 Structure report

The remainder of this report will be structured as follows. The next four chapters answer research questions based on a literature study. This literature study will help gain an understanding of the underlying problem and motivate the need for a solution.

In chapter 6 this background information will be used to further define the problem and define objectives for a solution. These objectives will be used in the same chapter to design and propose a solution for the identified problem. In chapter 7 we will describe a case study to demonstrate the proposed solutions. This case study will be executed at Welzorg. The results of this case study will be discussed in two chapters. First of all the practical implications for the organization at which the case study was applies. Chapter 9 will discuss the proposed solution based on the executed case study. Both are essential steps in the evaluation phase.

Finally, this report will end with a conclusion where the research questions will be answered and where some future work will be proposed.

2 Reference and Enterprise Architecture

In this chapter the concepts reference architectures and enterprise architectures will be explored. This chapter will cover a deep exploration of both concepts, techniques used and some examples of reference architectures.

2.1 Reference architecture

Before we explore reference architectures any further we need to have a some definition of what a reference architecture is. Multiple definitions are available. Nakagawa and Maldonado (2008), who focus purely on the software domain, define reference architectures as "artifacts that comprises knowledge of a given domain and support development of systems for that domain". The focus is purely on the development of new artifacts based on the reference architecture by sharing and representing knowledge in a certain domain. Greefhorst et al. (2009) studied several definitions and proposes to use the following definition: "A reference architecture is a generic architecture for a class of systems based on best practices" which is close to the definition used by Angelov et al. (2012): “A reference architecture is a generic architecture for a class of systems that is used as a foundation for the design of concrete architectures from this class”.

Aspects

Based on these definitions we can identify some important aspects of reference architectures. An important element of an reference architecture is that it should be generic. This says something about the level of abstraction. The reference architecture should be able to act as some kind of template with which detailed architectures can be developed.

The reference architecture can be used to design or analyze concrete architectures and should therefore be reusable. The reference architecture must be used for the design or analysis of multiple concrete architectures or class of systems and not be specifically designed for one system.

A reference architecture is an architecture and therefore contains some kind of structure as well as principles and guidelines of how this structure should be applied to specific implementations.

Reference architectures present generalized functions and configuration and therefore provide a reliable base for future developed architectures.

The domains covered by reference architectures can vary. Some reference architectures only focus on software architectures while other reference architectures take a broader scope and also take into account the technology, data and process layers and related architecture.

Classification

As can be derived from the broad definition of reference architecture there a many different types of reference architectures. Fattah (2009) rates reference architectures on two dimensions: the coverage of the reference architecture and the level of abstraction or detail. The coverage dimension is about the area or domain in which the reference architecture can be applied.

Angelov et al. (2012) designed a more extensive framework to classify the different reference architectures. It does so by scoring reference architectures on multiple dimensions, which are: context, goal and design. The context dimension focuses on where the reference architecture will be used and who defined it. The goal dimension scores a reference architecture on why it is defined: to standardize a group of solution architectures or to facilitate the design of it. And finally the design dimension which focuses on elements like the level of detail of the reference architecture, what elements are covered by the reference architecture and the way the reference architecture is represented. How a reference architecture scores on these dimensions defines the type of reference architecture, resulting in five possible types:

1. A classical, standardization reference architecture for multiple organizations
2. A classical, standardization reference architecture for a single organization
3. A classical, facilitation reference architecture for multiple organizations by an independent organization
4. A classical, facilitation reference architecture designed to be implemented in a single organization
5. A preliminary, facilitation reference architecture for multiple organizations (for future needs, other designed by a research center)

A classical reference architecture is defined as "a reference architecture that is defined when technology, software, and algorithms required for the architecture application exist by the time of its design and have been tested in practice" (Angelov et al., 2012). The classification of reference architectures helps to understand the different types of reference architectures. These classifications also helps the development and design of new reference architectures by giving a structured background.

Design

The framework proposed by Angelov et al. (2012) can be used to design new reference architectures. In (Fig. 2.1) an approach is shown of how to use the framework to design a new reference architecture. Using this framework should prevent poor initial chooses and failure of the design project and therefore saves time and money.

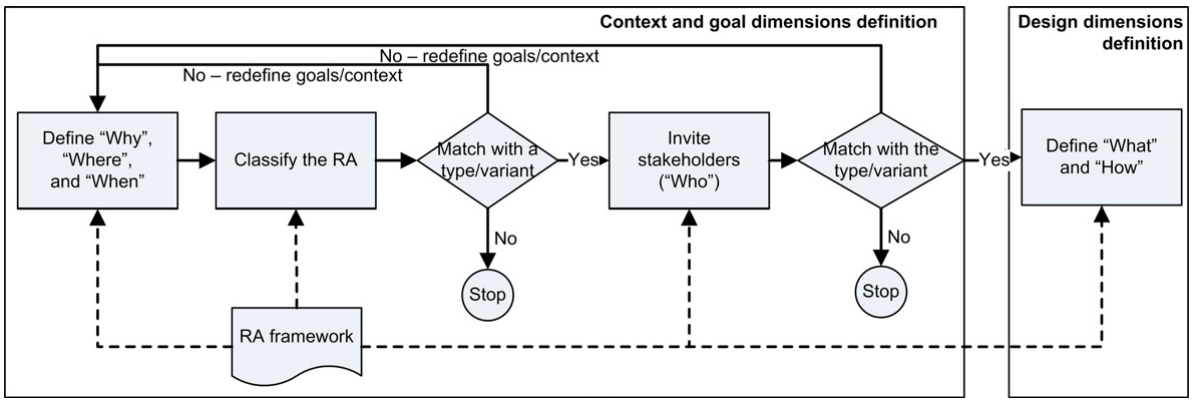

Fig. 2.1: Angelov et al. (2012) - Framework usage in the design of reference architecture

Cloutier et al. (2009) researched the driving forces between reference architecture. These driving forces are all input in a design process. The needs of the customer market, the opportunities that technology offers, the elaboration of the vision and off course the knowledge from existing architectures are all input when developing and maintaining a reference architecture.

Properly designed reference architectures facilitate reuse of domain knowledge and increase the interoperability between derivative systems. It thereby reduces the development time, risks, costs, and increases the quality of solution architectures. Using the classification helps to achieve this and makes sure all conditions for a successful reference architecture are met.

2.2 Enterprise architecture

Reference architectures are either a set of concrete architectures or used to design a specific implementation. Among other architectures these can be enterprise architectures. According to *ArchiMate*® (2017) an enterprise architecture is "a coherent whole of principles, methods, and models that are used in the design and realization of an enterprise's organizational structure, business processes, information systems, and infrastructure". An enterprise architecture can be seen as a blueprint for the whole organization and gives a holistic view of the enterprise. It relates all software and business processes to the mission of an organization. This definition makes clear that an enterprise architecture covers many levels in an organization. Often, there is a distinction made between the business processes, data, software or applications and the technological infrastructure.

Stakeholders, viewpoints and views

An enterprise architecture is a blueprint of an organization but will look different for different stakeholders since they have different interests. This is covered by an important set of terminology which is often used in enterprise architectures: the distinction made between stakeholders, their viewpoints, their views, and their concerns. In the ISO/IEC 42010 standard (ISO, 2011) these concepts are clearly defined together with the relation between these concepts. The stakeholder is an individual, team or organization having an interest in the system. This stakeholder has one or more concerns about the system. This results in a perspective on the system of interest called the viewpoint. The view is the representation of the system form a certain perspective or viewpoint. These concepts are illustrated in (Fig. 2.2).

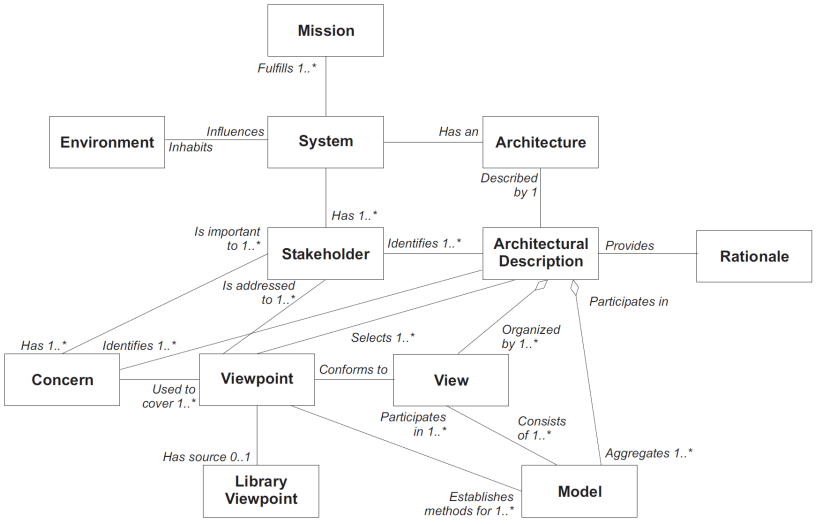

Fig. 2.2: ISO (2011) - Basic Architectural Concepts

Goals

But why should organizations want to have this blueprint of their organization? Having control over the complex business and IT inside an organization is ongoing challenge. An although enterprise architecture is not the holy grail it certainly is part of the solution. With an enterprise architecture organizations have more insight in this complexity and have more control over processes and IT part of their organization. Important is the integrated approach of business and IT, the alignment between these fields of interest. Organizations and their environments will constantly change and with an enterprise architecture you can keep track of these changes and respond quick and effective. With an enterprise architecture you can communicate about an organization's business, IT and goals in an structured an homogeneous way Iacob et al. (2012b).

2.3 Frameworks and methodologies

Multiple enterprise architecture frameworks and methodologies are currently available to support a structured design of enterprise architecture. Some popular frameworks are TEAF, FEAF, DoDAF, Zachman Framework and The Open Group Architecture Framework.

The Zachman Framework is one of the first of its kind and well known. The framework in its most simple form is a two dimensional classification scheme represented in a 6x6 matrix (Sowa and Zachman, 1992). The first dimension represents the perspective and the second dimension the abstraction. The Zachman Framework is purely a framework and not a methodology. No specific methods are described that define how information of the framework is used or how an instance of the framework is developed. Although the framework is easy to understand it isn't used in practice that often due to the large amount of classes it describes. But it helps to understand the concerns that should be covered by an enterprise architecture.

TOGAF

A frameworks that is quite popular nowadays and used in practice often is TOGAF (The Open Group, 2011). *The Open Group* (2017) published the first version of TOGAF in 1995 and has released updated versions of the framework since. TOGAF covers four domains that together form the enterprise architecture:

Business Architecture	defines the business strategy, governance, organization and key processes
Data Architecture	describes the structure of the logical and physical data assets and data management resources
Application Architecture	describes the individual applications, their interactions and the interactions with the business processes of the organization
Technology Architecture	describes the logical software and hardware capabilities that are required to support the business, data and application services

A core element of TOGAF is the Architecture Development Method (ADM). This is a methodology describes how to develop and manage the lifecycle of an enterprise architecture. ADM is an iterative development cycle divided into phases (Fig. 2.3).

Phases B, C, and D cover the development of the domain specific architectures. Phase C, the information systems architecture development, combines the data and application architecture.

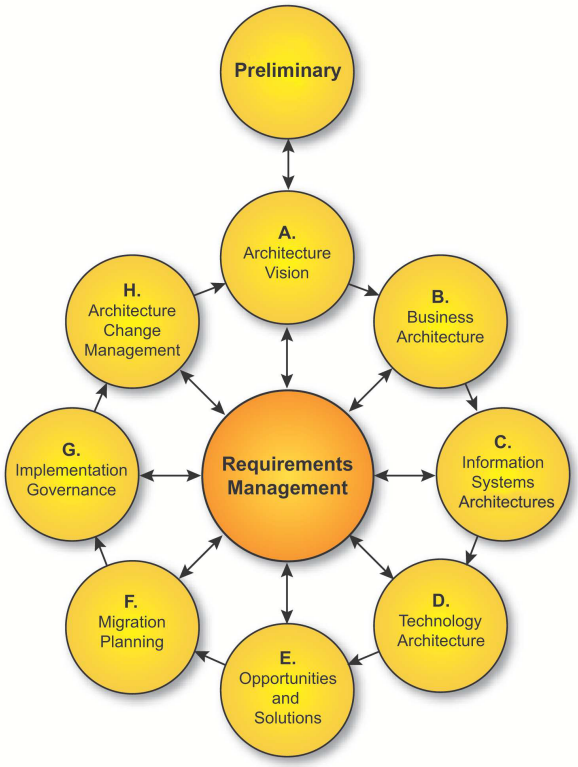

Fig. 2.3: The Open Group (2011) - Architecture Development Cycle

Another important element of TOGAF is the enterprise continuum. This continuum can be seen as a virtual repository with artifacts used to make communication about enterprise architecture easier and aid to organize re-usability of elements in an enterprise architecture. It provides an overall context for architectures and solutions. The continuum provides a classification for the assets in the enterprise repository.

Overall TOGAF is a framework based on best practices and structures the design and implementation of enterprise architectures. With ADM organizations can establish, develop, transition and govern their architectures. Results of the different phases of ADM can be stored in an architectural repository. The enterprise continuum helps to understand these architectural models.

Enterprise Architecture Modeling Language

TOGAF doesn't specify a specific modeling language with which the architecture can be described. However, ArchiMate is an open modeling standard which supports all phases of TOGAF ADM and is therefore a very suitable to use as modeling notation standard (Iacob et al., 2012b). ArchiMate (The Open Group, 2016) is a standard maintained by The Open Group and currently at version 3.0.

ArchiMate is a visual language which can be used to describe, analyze, and communicate enterprise architectures. The core of ArchiMate includes three layers: the business, application and technology layer. A second dimension of the ArchiMate core framework consists of three aspects: the active structure aspect which are the structural elements that display the actual behavior, the behavior aspect which represent the behavior performed by actors, and the passive structure aspect that represent the elements on which the behavior is performed. (Fig. 2.4)

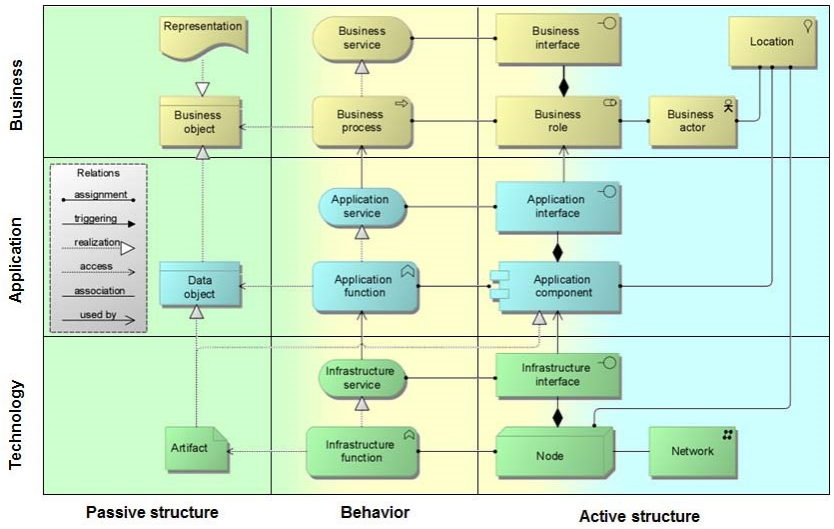

Fig. 2.4: Iacob et al. (2012a) - Simplified ArchiMate metamodel

The core of ArchiMate can be extended to cover more layers and aspects. The motivational aspect can be added to cover the motivations, or reasons, that guide the design of an enterprise architecture. An implementation & migration layer can be added which adds the ability to add projects in ArchiMate enterprise architecture models. These two extensions make that ArchiMate fully covers TOGAF ADM and make it an appropriate language with can be used in each phase as notation language (Fig. 2.5).

2.4 Examples

In this sections some reference architectures are highlighted. The Dutch reference architectures NORA, GEMMA and AORTA are introduced. A description is given about their goal and how they try to reach this goal.

NORA

The Dutch Government Reference Architecture (*Nederlandse Overheid Referentie Architectuur* 2017, NORA) is a reference architecture focusing on the whole Dutch public sector, including all domains and levels of governments. The core of NORA is a meta-model describing relevant architectural elements. First of all this meta-model describes the policy framework. A set

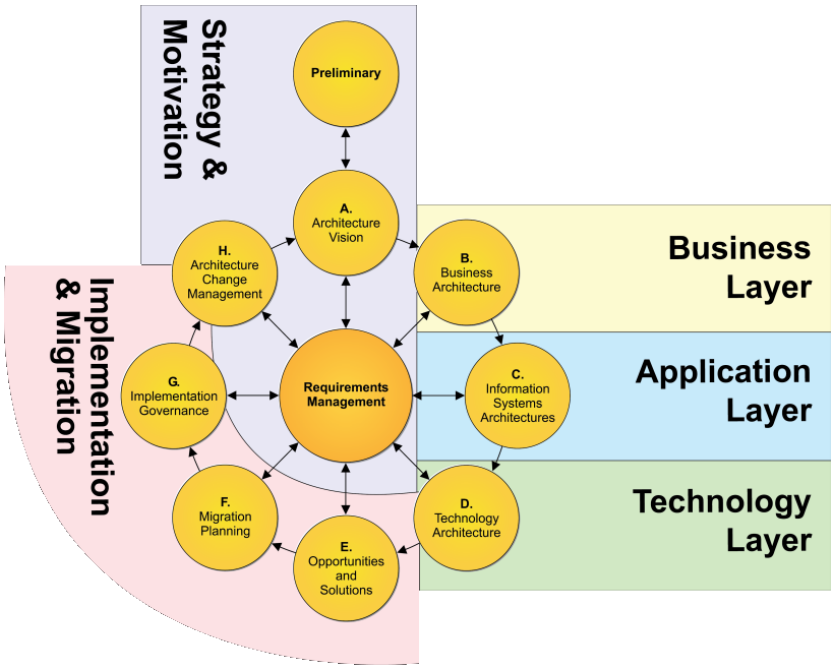

Fig. 2.5: The Open Group (2016) - TOGAF ADM and the ArchiMate framework

of 10 basic principles and about 40 derivative principles is derived from the policy elements. Based on these principles some standards or building blocks can defined that support the principles. The main goal of NORA is to facilitate collaboration and information-exchange between different levels and domains of government. The NORA family is a set of reference architectures and enterprise architectures that that cover certain public domains or levels of government. NORA uses the standards ArchiMate and TOGAF as much as possible to describe the architecture and architectural elements.

Although NORA primarily focuses on the public sector, the reference architecture is also interesting for private organizations that want or have to connect with the public domain (Greve, 2016). NORA is missing detailed solutions in the technical architecture domain. However, on an organizational level NORA provides a solid basis for solution architectures and gives a common communication language.

GEMMA

An extensive reference architecture which is part of the NORA family is the Dutch Municipalities Model Architecture (*Gemeentelijke Model Architectuur* 2017, GEMMA). GEMMA covers a single level of government, the municipalities. The development and maintenance of GEMMA is governed by *KING* (2017) and the current version covers the whole organization of municipalities. The GEMMA meta-model is based on ArchiMate. The business and application layer are well defined and cover the business functions, related application function and application components that are typically carried out by municipalities. Furthermore, data and message standardization is incorporated in the reference architecture. A clear advantage of the refer-

ence architecture are these standards. A clear advantage for municipalities is the use of these standards since this prevents a vendor lock. Software suppliers that develop applications for municipalities can use GEMMA to classify the functions covered by the application.

AORTA

AORTA (*Architectuur AORTA* 2016) is a national infrastructure to exchange health care information. AORTA describes the architecture around an central application (Landelijk Schakelpunt, LSP) which coordinates the exchange of health care information between care givers. AORTA is also part of the NORA family.

AORTA describes a decentralized implementation of an electrical health record system. The central application, the LSP, doesn't store any medical records but instead redirects requests for medical records to the care system that can provide the information. These care systems are the systems used by the health care providers to store medical information of clients. AORTA describes all principles, business processes, applications and interfaces that make the information exchange possible and save. An important set of artifacts of AORTA are the communication standards. These are used for the authentication, authorization, information exchange and error messages.

2.5 Summary

A reference architecture is a generic architecture used to design or concrete a single solution architecture in a certain area of interest based on a class of systems. This can either be preliminary to the development of the development of solution architectures or be based on current solution architectures. Reference architectures facilitate the reuse of domain knowledge by providing guidelines, principles and some kind of structure.

Enterprise architectures are a blueprint of an enterprise by describing the organization, business processes and information technology used. Different stakeholders have different interest which can be addressed by different views on the enterprise architecture.

TOGAF is a framework describing a methodology that can be used to develop and manage an enterprise architecture. ArchiMate can be used as a modeling language for enterprise architectures. The TOGAF ADM and ArchiMate modeling language supplement each other since ArchiMate covers each activity of the ADM cycle. Both are used to describe elements of reference architectures like NORA and GEMMA.

3 Risk Management and Regulatory Compliance

In this chapter risk management, regulatory compliance an integrated approach covering governance, risk and compliance will be examined. The important concepts and taxonomy used will be covered as well as some standards used and well known methodologies. All to have a better understanding of these concepts.

3.1 Regulatory compliance

First of all we need a definition of what compliance is. Sadiq and Governatori (2010) define compliance as follows: “Compliance is defined as ensuring that business processes, operations, and practice are in accordance with a prescribed and/or agreed set of norms.” These sets of norms can consist of requirements that are a result of national or international legislature, rules of regulatory bodies, standards and codes from the industry and even regulations that are a result of the contracts with business partners. A company or organization is called compliant when all the compliance requirements are fulfilled.

Motivations

But why would an organization be compliant? Being compliant is often seen as a burden (Sadiq and Governatori, 2010). Besides, not being compliant with regulations and rules can have some advantages. Sutinen and Kuperan (1999) came up with a social-economic theory about regulatory compliance (Fig. 3.1). In this model they combine the economic, social and psychological theories to show the motivations of why to be compliant. There is often an financial incentive, illegal gain, not to be compliant. On the other hand there can be an expected penalty or fine enforced by a government or other instance that have a deterrence. Finally there is a moral obligation and social influence that motivate people to the greater or lesser extent to be compliant. Most people have the instinct to follow the rules of authorities they have accepted. And the other important social factor is the external pressure, where the social reputation is at stake.

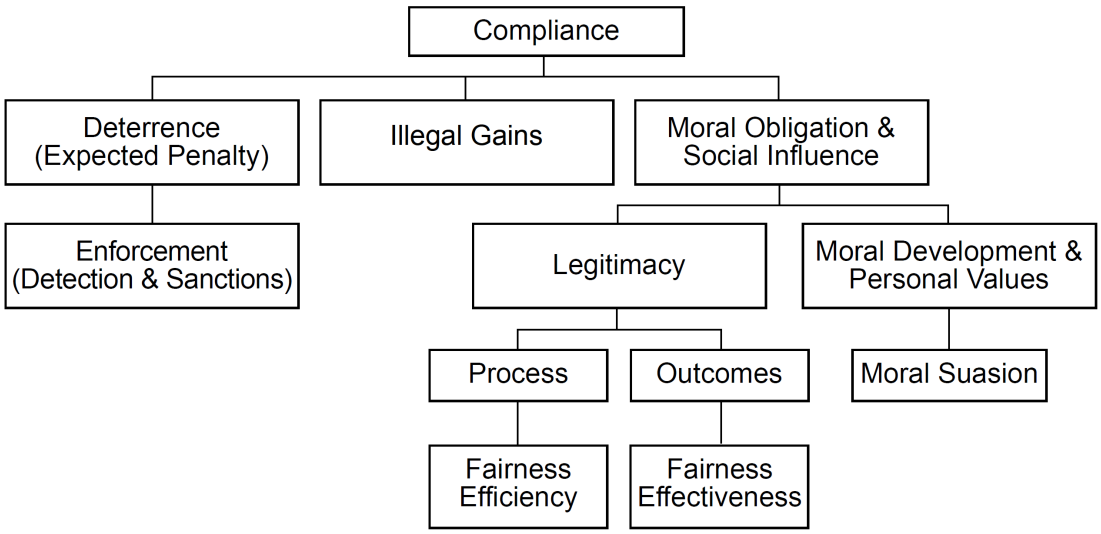

Fig. 3.1: Sutinen and Kuperan (1999) - Determinants of Compliance

Challenges

It can be challenging for an organization to be regulatory compliant. Syed Abdullah et al. (2010) recognize challenges in three categories: customer related, regulation related and solution related. In organization there can for example be a lack of compliance culture while this is an important factor in achieving regulatory compliance. Another important factor is whether an organization has efficient risk management. This is also related to the cultural factor; there has to be a willingness to put effort in the management of the existing risks.

Organization also tent to see only the negative side of regulatory compliance and have a lack of perception of compliance as value-add. On top of this high costs of implementing a compliance framework can indeed temper the advantages. But more and more organizations see the obligation to comply as an opportunity to redesign and improve their business processes (Sadiq et al., 2007). But there are also some regulation regulated challenges. Regulations tend to change fast. This makes it hard to keep compliant. Sometimes regulations are inconsistent with each other or even conflict. Furthermore, high level specified regulation can lead to miss interpretation.

Employees are often seen as the weakest link in information security. This makes the understanding of the behavior of employees regarding compliance crucial in order to become regulatory compliant. Bulgurcu et al. (2010) developed a model which captures the factors that influence the employees attitude towards compliance (Fig. 3.2). An important lesson is that a security-aware culture within an organization improves the information security. The intention to comply of employees can be influenced by creating security awareness. Training

employees also contributes to a information security since employees have a self-efficacy to comply.

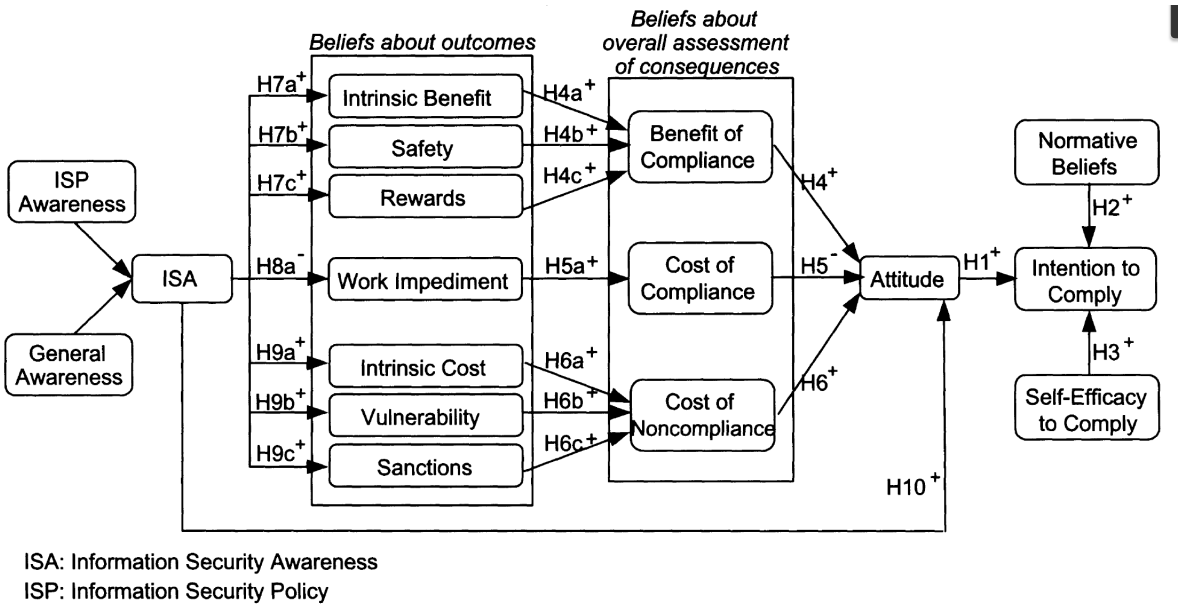

Fig. 3.2: Bulgurcu et al. (2010) - Model of the Antecedents of ISP Compliance

Two challenges stated earlier that make being compliant unsustainable are the constant changing regulations and the inconsistency between regulations. Sadiq et al. (2007) also recognize this velocity and also identify inconsistency between regulations and business requirements. Business Process Management and Controls Management are two work fields that heavily interact with each other (Fig. 3.3). This shows that when a redesign takes place the risk assessment should be updated as well. Or an updated control mechanism should impacts the way a business process is executed. This can for example be an updated compliance requirement which captures an object an organization has to fulfill in order to be compliant.

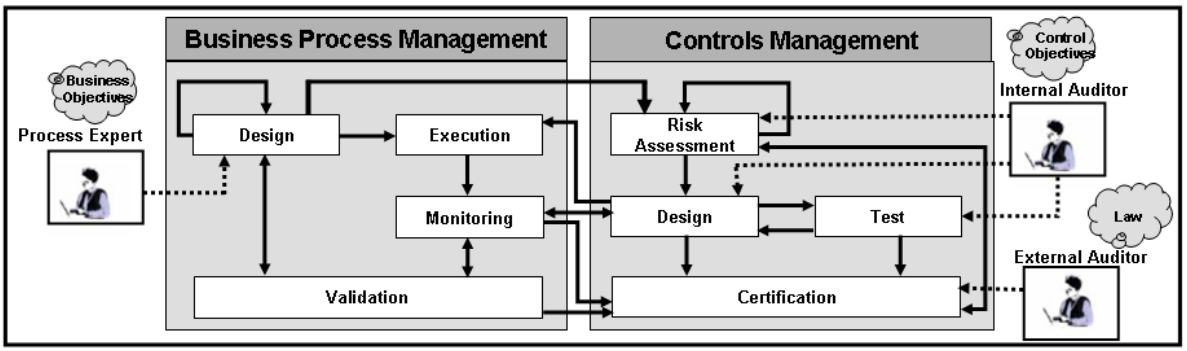

Fig. 3.3: Sadiq et al. (2007) - Interaction between Process Management and Control Management

3.2 Risk management

Risk management is a about identifying, assessing and prioritizing risks. First of all the taxonomy of risk will be explained, followed by a mapping of this taxonomy on enterprise architectures. Finally some standards are discussed used to standardize risk management.

Risk assessment

There are a lot of different methodologies, methods and tools available to do risk assessments with (Ionita, 2013). These methodologies share common fundamental concepts that define risk. The taxonomy used in the mayor risk frameworks include:

Threat Initiates an attack

Asset The target (physically or digital) of a possible attack

Vulnerability A weakness of an asset, for example a flaw in the design or implementation but also possibly in a policy or business model

Attack The actual event where a vulnerability of an asset is exploited and therefore initiates a threat

The risk is often decomposed into two factors: the frequency or likelihood of a loss event and the magnitude or impact of a probable loss event. The likelihood times the impact results in a calculated risk.

In risk assessment methodologies and frameworks these risk concepts are used to evaluate the risk associated with a system. In the Information Technology field it is used to identify, monitor and control the risk associated with Information Systems. A risk assessment is an activity that is executed when required in a typical Risk Management process. All popular methodologies follow a common formula (Ionita, 2013):

1. Establishment of context
2. Risk Identification
3. Risk Analysis
4. Risk Evaluation
5. Select countermeasures

Risk and security are strongly related. The results of a risk assessment can be used to make new or update security requirements. A risk assessment can also be used to evaluate the risk

related with the existing security requirements. You can either focus on existing gaps in the existing security (a gap analysis) or use the analysis to show compliance with the active security regulations.

Risk and Security in Enterprise Architecture

Enterprise architectures describe business processes, applications and technology used in organization. These elements can all be exposed to greater or lesser extend to threats. Band et al. (2015) present an extension for the ArchiMate modeling language to cover risk and security aspects. This ArchiMate extension uses the risk concepts as defined earlier, resulting in a mapping of risk concepts onto the ArchiMate core according to (Fig. 3.4). Not only are the risk elements mapped but also elements of possible countermeasures. This makes this mapping useful during the whole execution of a risk assessment methodology.

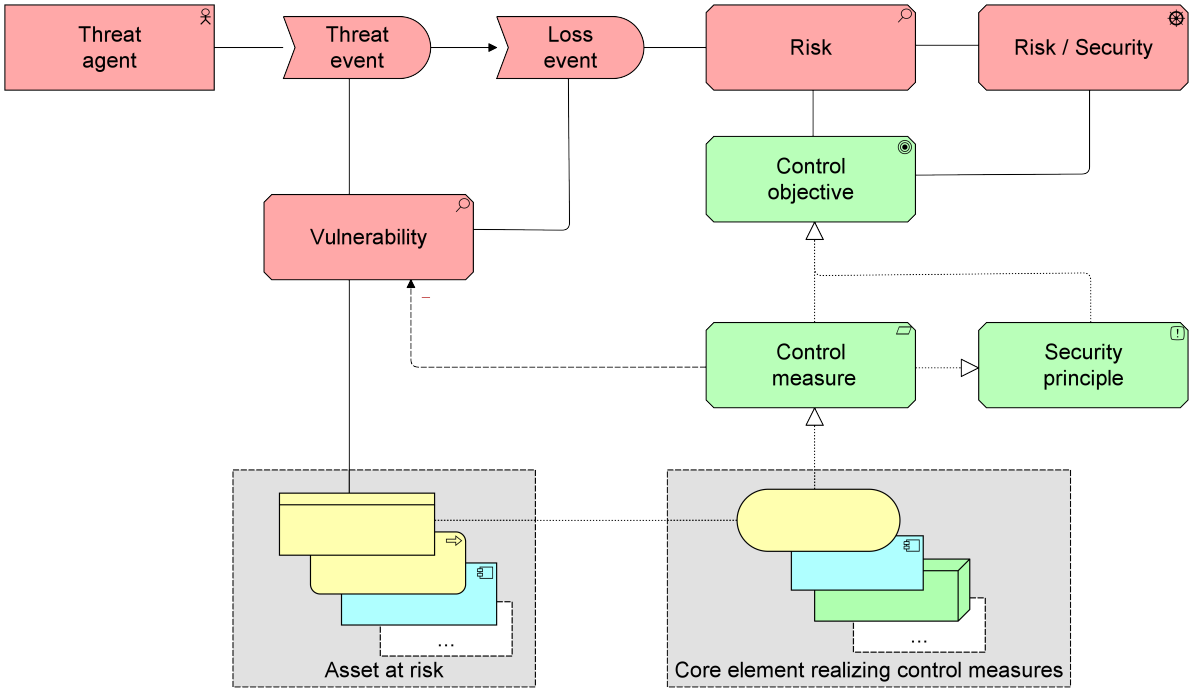

Fig. 3.4: (Jonkers, 2014) - ArchiMate Risk Concepts Mapping

But enterprise architecture management and security risk management also complement each other the other way around. Mayer et al. (2015) suggest that proper enterprise architecture management can improve the security risk management when both domains are integrated together. Risk assessment methodologies have difficulties with modeling the assets at risk. With enterprise architecture methodologies this can be a problem of the past. An integrated approach of risk management an enterprise architecture management gives enterprise architecture even more value to develop and maintain and gives risk management methodologies tools to model assets, risks and countermeasures.

Standards

Different standards are developed to help organizations establish, implement and/or maintain a certain level of security to reduce risk. These standards give a taxonomy of risk and specify how to reduce risk. The International Organization for Standardization (ISO) has published a whole family of standards that can be used to establish an environment where information is protected. The ISO 27000 is a family of standards covering information security practices and is based on best practices (Deiters et al., 2009).

The ISO/IEC 27001 (2013) specifies an information security management system. It specifies the requirements must be fulfilled in order to be compliant with the standard. One main requirement is having a Plan-Do-Check-Act (PDCA) oriented security management approach. Establishing (Plan), implementing (Do), monitoring, (Check), and maintaining and improving (Act) the information security management system (ISMS) is the main objective of ISO 27001. Risks should be identified and assessed and control objectives should be defined to reduce the risk. ISO 27001 comes with a list of control objectives for security management.

ISO/IEC 27002 (2013) is a more expanded and contains further explanation compared to ISO 27001. It gives guidelines for organizational information security standards and a more detailed explanation of the control objectives described in ISO 27001. The controls furthermore cover security guidelines, access control, human resource security, physical security and information systems security.

ISO/IEC 27799 (2016) is a standard specially developed for the health care industry. It is based on the guidelines as described by ISO 27002 and supplemented with sector specific requirements. The Dutch NEN 7510 (2011) standard is based on ISO 27799 and is further adjusted to fit the Dutch health care system and Dutch regulations. Secrecy, availability, integrity and privacy are important requirements in the health care industry covered by this standard. Applying the guidelines described by NEN 7510 results in an environment compliant with these requirements.

Together these standards bundle the practical knowledge and the state of the art regarding information security. These standards can be used by all kind of organizations, although ISO 27799 is specific covers the health care industry. Organizations can be certified regarding these standards, meaning they have implemented information security controls as specified by these standards.

3.3 Governance, risk and compliance

Regulatory compliance and risk management are subjects covering partly the same field of interest. Together with governance they have been a subject of research for some time now under the umbrella term: governance, risk and compliance (GRC). One of the first studies mentioning the subjects together is Humphreys (2008). This research focuses on insider threats, an employee that tries to do harm for example by stealing information. It argues that correct governance should be in place together with an effective risk management process to mitigate the threat and reduce the risk.

The individual concepts itself aren't new. In previous sections of this paper the concepts risk management and regulatory compliance are examined. What is new is attention for the integrated approach regarding GRC. Individual concepts are shared between the fields governance, risk and compliance. Racz et al. (2010) tried to catch these shared concepts and made a high level frame or reference for an integrated GRC. This results in the following definition: "GRC is an integrated, holistic approach to organization-wide governance, risk and compliance ensuring that an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations, through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness."

Conceptual modeling is used by Vicente et al. (2011) to define the domain of integrated GRC. By investigating the taxonomy used and visualize the concepts in a model the shared elements become clear. In (Fig. 3.5) the model is shown and all shared concepts are included. It shows how governance, risk and compliance are linked to each other and effect each other. Four concepts are identified as the core of integrated GRC since they are shared by all three terms. Internal controls, processes, risks and policies are the crucial concepts defining GRC.

To make this conceptual model more usable for practice and the understanding more general available Vicente and Silva (2011) developed a reference architecture. This reference architecture is a specialization of the reference model and modeled with the modelling language ArchiMate. This modeling language is used since it is well-accepted and is able to cover both the business and the IT. Four viewpoint are used to illustrate the GRC reference model. The application structure view as shown in (Fig. 3.6) shows application components and associated information assets. The result is similar to the representation of the concepts in (Fig. 3.5) but modeled in a language that is well accepted. The result is a reference architecture for governance, risk and compliance.

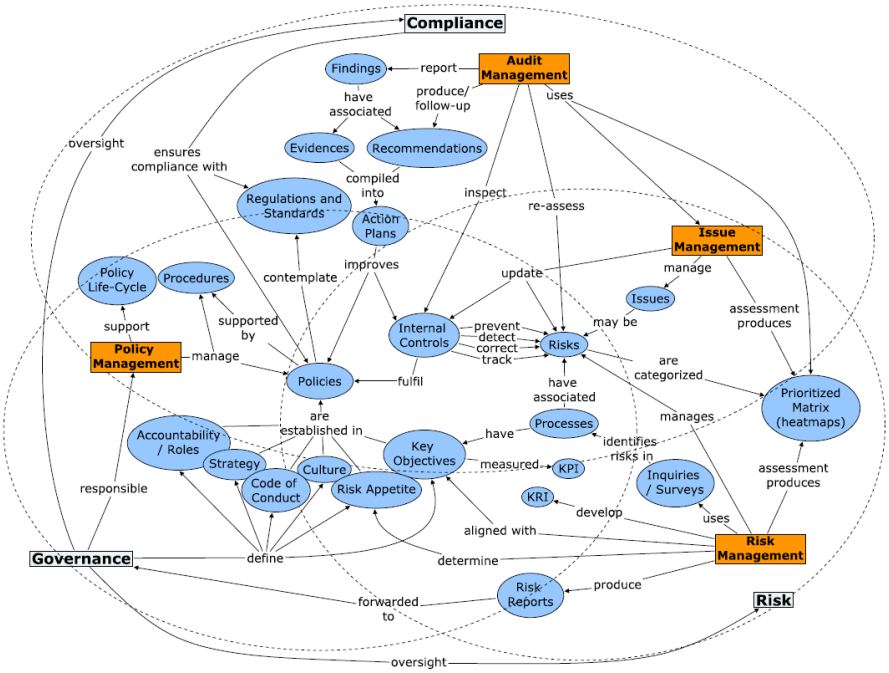

Fig. 3.5: Vicente et al. (2011) - Integrated GRC Conceptual Model

3.4 Summary

Regulatory compliance is about complying with rules, regulations and standards. The drive to be compliant or not is driven by (financial) sanctions, illegal gains or social and moral factors. Continues compliance management is needed since both the regulations change over time as well as the environment that should be compliant.

The concept risk can be broken down to frequency of an possible attack and the impact of such an attack. An attack is initiated by a threat that uses a vulnerability of an asset. Many risk management methodologies are available, all covering the establishing of the context followed by the identification, analysis and evaluation of the risk and finally the selectmen of counter measures. Multiple standards are available based on best practices that, when applied, make sure your organization deals with risks appropriately.

Regulatory compliance and risk management share, together with governance, many concepts. Internal controls, some of which are the result of the will to be compliant with regulations or standards, try to reduce the risk. Risk management methodologies are developed to identify and address risks in processes. Once compliant with standards like ISO 27001 the risk in an organization is addressed in an appropriate way. However, these standards don't state how to be compliant since this differs for every organization.

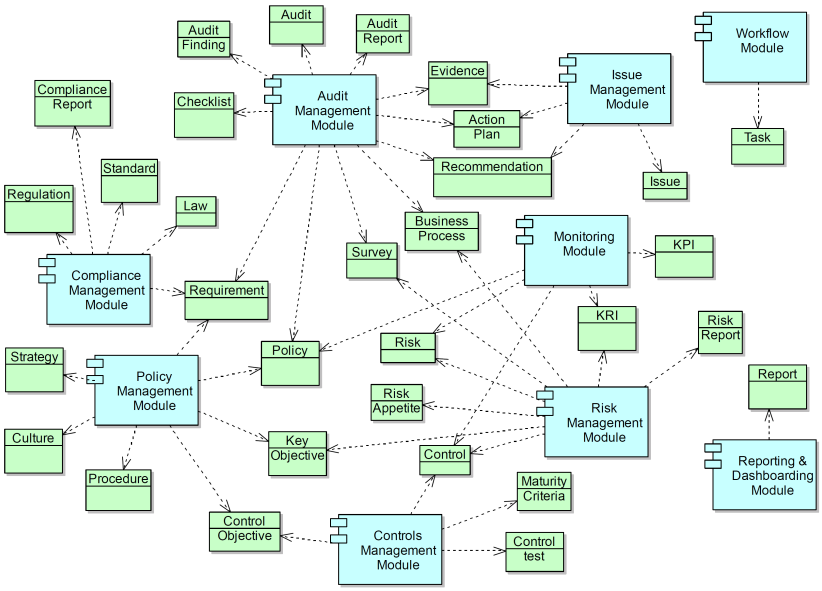

Fig. 3.6: Vicente and Silva (2011) - GRC RA Application Structure Viewpoint

4 Privacy

To understand why privacy regulations are important you have to understand what privacy is and why privacy is important. First of all the concept privacy will be covered. Next, privacy regulations are covered by this research. Both the Dutch WPB which currently protects individuals privacy and the successor GDPR are examined. This chapter also covers regulations regarding the Dutch national identification number. This unique number is often treated as special personal information.

4.1 Privacy explained

What does privacy entail? Privacy is broad concept covering many areas of interest. For example, freedom of thought, control over one's body and control over personal information are topics affiliated with privacy (Solove, 2008).

Privacy is a social concept. It's about feeling safe and trusted by others. Fried (1968) define privacy as a matter of who has control over personal information, information about ourselves. The right of privacy and the reason why you people are hurt when this right is invaded are discussed by Fried. Laws and regulations are required in modern societies to give someone control over his own personal information.

Solove (2006) has defined a taxonomy for privacy consisting of four groups of activities. These groups of activities cover different actions that can affect someone's privacy. The four groups are: information collection, information processing, information dissemination and invasion. In (Fig. 4.1) the groups of activities are illustrated together with the specific activities that can violate someone's privacy.

The first group of activities, the collection of information, can violate someone's privacy in two ways. Surveillance and integration are two different activities of information collection. For surveillance, someone doesn't have to publish any kind of information and even be aware that personal information is collected. Interrogation covers all activities where a person is questioned, even inoffensively.

Information processing covers all activities that somehow process or handle the personal information that is collected. It covers aggregation of information (bringing together information),

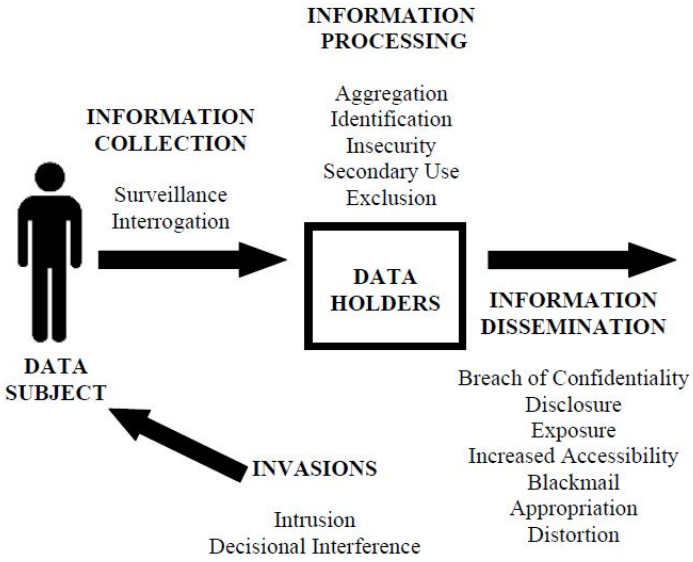

Fig. 4.1: Solove (2006) - Privacy Taxonomy

identification, insecurity of the stored information, secondary usage of data (usage other than the purpose it was collected for) and the exclusion of an individual when processing his personal information.

Information dissemination is the broadest group of activities. It covers activities where the personal information that is processed at a third party is somehow under attack. This can by a breach of confidentiality, by disclosure, by exposure, by an increase of accessibility, by blackmailing, by appropriation, or by distortion.

Finally, Solove (2006) recognize a group of activities labeled invasion. This covers the activities intrusion in someone's live and decisional interference when a choice has to be made that concerns someone's autonomy.

The origin of privacy maybe an individual's "desire to avoid having his/her personal information used to harm him/her" (Hughes, 2015). Privacy is having control over your own personal information and thereby reducing the possible harm that can be caused by having too much personal information publicly available or under the control of others.

Summarizing, it is important to understand privacy is about having control over personal information. The exposure of personal information can effect someone´s trust and confidence. The taxonomy as defined by Solove (2006) ca be used to understand the different types of threats regarding privacy.

4.2 Privacy regulations

As stated in the previous section, laws and regulations are needed to protect personal information. Giving citizens the legal rights regarding their personal information is one way to ensure privacy is dealt with correctly. Many countries therefore have regulation that protect personal data. The Dutch Data Protection Act (*Wet bescherming persoonsgegevens* 2000) ensures the protection of personal data of individuals in the Netherlands. This act is based on an European directive. The WBP will be replaced by a European regulation in 2018. The General Data Protection Regulation copes better with the challenges that come with automated data processing and will introduce a single level playing field in Europe regarding privacy.

4.2.1 Data Protection Act (WBP)

The WBP regulates the collecting and processing of personal data, both the automated processing of data as well as the non-automated processing. With the processing of the data the broadest definition is used: collecting, capturing, arranging, storing, changing, requesting, consulting and the usage of personal data are all covered by the WBP.

The law makes a distinction between the responsible and the processor of personal data. The responsible natural or legal person is the one who determines the goal of and the means for the collection of personal data. The processor is whom processes personal data for the purpose of the responsible and isn't directly subject to his authority.

The responsible makes sure that the processing of personal data only happens on behave of the responsible. Besides, suitable technical and organizational measures should be in place to protect the personal data.

A special set of personal data which is explicitly mentioned in the Data Protection Act is personal data concerning someone's religion or believes, race, political orientation, health, sexual orientation, or trade union membership. The processing of this special set of personal data is explicitly prohibited.

There are some exceptions on this prohibition. These exception are explicitly mentioned in the WBP and are almost always related to the necessity of an organization or government agency to be able to carry out its task. For example, hospitals and other health care organizations need health related personal information to be able to select the best treatment possible.

The collecting and processing of personal data has to have a legal basis or the concerned person should have signed an unambiguous agreement stating the purpose of the collection. The second option is often the case when someone agrees with a sales agreement or an user

agreement. The legal basis for the collection of personal information in the health care industry is regulated in the health care acts.

The processing of personal data is always limited to the purpose of the collection of the personal data. This means that when organizations have collected personal data, the data should only be used for the purpose it was collected for. The processing of the information should always happen carefully and safe. Appropriate security measures should be in place to ensure this.

The organization processing the personal information should make sure the data integrity of the personal information by making sure the data is correct and accurate. The data should never be stored longer than needed on no more data than required to execute operational processes may be stored.

The WBP also contains measures in case of an offence. First of all is every organization processing personal information obligated to report a privacy leakage. This, for example, can be the case when an email with personal information is send to wrong email address. Or when a USB containing client files is lost. The report has to be made to the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens* (2017)).

The concerned one also has certain rights regarding their personal information. They have the right to know why and which data is collected and stored. They have the right to correct the data that is collected, to resist collecting and processing when legal basis and finally the right to be forgotten. Organizations collecting and processing personal information have to take into account these rights and comply with these regulations by designing processes that allow clients to execute their rights.

4.2.2 Dutch National Identification Number (BSN)

The Dutch National Identification Number (*Wet algemene bepalingen burgerservicenummer* (2007), BSN) is a unique identification number used by the Dutch government. The BSN explicitly isn't considered as personal information and the number doesn't contain any information about the person it is assigned to. Nevertheless is the BSN used to uniquely identify a person and is the BSN threaded as a special personal information element.

The BSN is primarily and exclusively used by governmental organizations in the communication between governmental institutions and between the concerned citizen and the government. The act regarding the BSN excludes any other usage of the BSN, except a few exceptions. These exceptions are clearly defined in other acts.

For the use of personal data in the health care industry there is a separate additional law, the Additional Act regulating Privacy in the Health Care Industry (*Wet aanvullende bepalingen*

verwerking persoonsgegevens in de zorg 2017). This act explicitly covers the health care as described by the WLZ and the ZVW and doesn't cover the health care by the WMO.

The above act regulates the usage of BSN in the health care industry. Using the BSN in the health care industry should prevent mixing up clients and reduce fraud. A health care provider is required to check the identity of all clients and send a bill to the health insurers based on the BSN. The use of the BSN is limited by the acts as referred to above. Any collecting or processing of the BSN without statutory provision is not allowed.

4.2.3 General Data Protection Regulation

The *General Data Protection Regulation* (2016) (GDPR) is a new European directive that becomes active in May 2018. This law will replace local data protection laws in the European countries, like the Dutch WBP. These new regulations make sure that in every European country the level of protection. This should make it easier for organizations that operate in multiple European countries since they only have to comply to one set of privacy regulations, one level playing field. A second reason to introduce new regulations is the still growing automated data processing. The introduction of information systems and computer networks made the processing of data, and therefore privacy sensitive data, easier. The new regulations try to cover the challenges that come with this change.

The GDPR can be seen as an expansion of the WPB: the privacy rights for citizens are reinforced and the responsibilities of organizations are expanded. Almost everything regulated by the WPB stays at least the same. The same distinction is made between the responsible one and the processor. The processing of a special set of personal information is still explicitly regulated. The new regulations of the GDPR can maybe be best summarized as more restrictions and obligations for organizations processing personal information and more rights for the citizens who's personal information it concerns.

For organization the new regulations focus more on their accountability regarding the processing of personal data and demonstrating compliance. An important requirements is to show the purpose of the collecting or processing of personal information. Any processing other than the purpose it is collected for is prohibited.

This results in the requirement for organizations to document their organizational and technical measurements to show they comply with the GDPR. On top of this, some organizations need to execute a Privacy Impact Assessment (PIA) and need to appoint a data protection officer (DPO).

Privacy Impact Assessment

Organizations that perform one of the following activities are obligated to execute a PIA:

1. Systematically evaluate personal aspects (like profiling)
2. Process special personal data on a large scale
3. Track person in public area on a big scale and systematically

A PIA is an instrument to map out the risks that comes with the processing of the personal data and to show the measurements to reduce these risks. A PIA should ideally happen before any personal information is processed by an organization. The assessment should be focused on the necessity and proportionality of the operations using personal information. A PIA should make clear what the critical operations are and which control measures are installed to reduce the risk of losing personal information. Tools that can be used to execute a PIA create awareness about the state of protection regarding privacy by the execution of a questionnaire. The goal of the execution of a PIA is an organization that has implemented privacy by default and design.

Data Protection Officer

An organization should assign an DPO when the processing of personal information:

1. is done by a government agency
2. is done systematically and on a large scale
3. covers special personal data

A DPO has to have a good understanding of the applicable privacy rules and regulations. The person that is assigned as DPO of an organization doesn't have to be an employee of the organization, a legal company or a consultancy firm can fulfill this task. The DPO should however always be available for employee to answer questions regarding the processing of personal information.

A DPO is the first point of contact for all privacy related issues. He should have full access to all operations and operators that process personal information. He has a good understanding of the processes that require the personal information and the underlying infrastructure used to process all this information. He informs the organization about how the organization should comply to the GPDR and conduct internal audits to check whether the organizations complies. When a PIA is required the DPO advised regarding this matter.

Citizens' Rights and Sanctions

The GDPR gives individuals more rights regarding their personal information. The rights are further strengthened in comparison to the rights as stated in the WBP. To protect these rights the sanctions that are imposed when an organization isn't compliant with the GDPR and violates the rights of individuals are significant. Besides written warnings and obligated regular data protection audits the GDPR also allows fines up to 20 million euros or 4% of the annual worldwide turnover of a company, whichever is greater.

Besides, privacy leakages tend to generate a lot of bad attention which could damage the reputation. Besides, nowadays the impact of a leakage is often is enormous. A leak often doesn't contain the information of only one individual but a whole set of personal information. Many individuals are affected by only one leakage due to the usage of information technology to efficiently process the information.

4.3 Summary

Privacy is a concept which is difficult to define. It is a social concept, it is about feeling safe and trusted and having control over your own personal information. Different types of threats can be defined that influence this feeling negatively. Invasion of your privacy, the collection, processing and dissemination of personal information all affect privacy.

Rules and regulations are needed to protect privacy. These give individuals rights regarding their own personal information and some control over the processing by others. In the Netherlands the WBP regulates the collecting and processing of personal information. This law dictates that organization, both private and public, should have either a legal basis for the processing or the subject should have given explicit permission for the collecting and/or processing. Besides, the processing of personal information is only allowed for the goal it was collected for.

The European GDPR is a directive that replaces privacy acts in the European countries. GDPR takes into account modern threats that could damage someone's privacy. The GDPR can be seen as a more strict act than WBP with more obligations for organizations processing personal information. In order to be compliant with these new regulations that become active in 2018 many organizations should evaluate how to adjust their processes to become compliant. Among other changes this means some organizations need to install a DPO and some need to execute a PIA.

Dutch Health Care System

5

Although most developed countries have some form of public health care there are huge differences between the way these are funded and what kind of services are covered by the public health care. The Dutch health care system is regulated by four laws (Ministerie van Volksgezondheid, Welzijn en Sport, 2016):

1. Health insurance act (*Zorgverzekeringswet* (2005), ZVW)
2. Long-term care act (*Wet langdurige zorg* (2014), WLZ)
3. Social support act (*Wet maatschappelijke ondersteuning 2015* (2014), WMO)
4. Youth care act (*Jeugdwet* 2014)

We are only interested in the first three laws since the Youth care act doesn't cover the financing of any kind of medical supplies. In the following paragraphs the act will be further explained, what they cover, who is responsible for the execution and how it is financed.

5.1 Health insurance act (ZVW)

Every Dutch citizen is required to have a basic health insurance. In the Netherlands 24 health insurances are offered by 9 health insurance companies (NZa, 2017). The four biggest health insurance companies cover over 88% of the market in 2017. The companies operate in the private sector. Depending on the income, citizens are entitled to an insurance's allowance to pay for their health insurance. For solidarity reasons, health insurers are not allowed to reject clients. To raise some awareness among citizens about the costs of health care, besides the insurance premium there is a obligatory deductible excess.

The health insurance covers about 60% of the total Dutch heath care budget. The basic health insurance covers the curative heath care like: GPs, hospital stays, drugs, short-term mental health care, and selected medical supplies and equipment. The ministry of public health publishes a detailed list of which health care is covered by the basic insurance.

When someone receives care from a health care provider the bill will go directly to the insurer when the provider is contracted by the insurer. Otherwise, the bill has to be paid in advance by the client who can then, when the service is covered by his insurance, invoice at his insurer. To simplify the execution and invoice process some health insurance companies have established

an organization: *VECOZO* (2017). VECOZO is currently the communication point for the health care industry. All health insurers are connected with the VECOZO communication hub and many care providers are.

The communication with the VECOZO communication hub is standardized. Standards as defined by *Vektis* (2017) are used for the communication. Different standards are available that standardize the possible communication and declaration messages. Beside the declaration messages an important standardized message is the so called 'VECOZO check' to check whether an individual has health insurance or not and which health care is covered.

5.2 Long-term care act (WLZ)

The long-term care act covers care for people who permanently need some form of care. Chronically ill, elderly or people with long term disabilities have the right to receive health care based on this act.

A needs assessment by CIZ indicates which persons have the right to receive which kind of care. A local health care office (Dutch: Zorgkantoor) takes care of the people that have a WLZ needs assessment. These health care offices have contracts with specialized health care facilities, home care institutions, nursing homes and other health care providers. In the Netherlands there are 31 health care offices executing the WLZ in their region.

The act covers the medical equipment used in these health care facilities. Sometimes these facilities need specialized equipment for certain clients. The WLZ act covers these kind of expenses.

5.3 Social support act (WMO)

The WMO covers the care for people with (minor) physical or mental disabilities. This act covers care like informal care support, household support, day care, and medical supplies and equipment. The group of medical equipment covered by the WMO are mobility solutions. Mobility aid equipment like wheelchairs, mobility scooters and adjusted bicycles are the main products covered by the WMO.

The WMO is executed by the municipalities. People who are eligible support based on the WMO go their municipality. The municipality reviews the application and selects in consultation with the client the care needed. The municipalities have contracted different health care provides that can provide the care covered by the WMO. The health care providers get the order from

the municipalities to supply their health care services to a client. Municipalities are free to contract one or more organization to deliver the WMO equipment.

Dutch municipalities are united in the *VNG* (2017) (Vereniging voor Nederlandse Gemeenten). The VNG supports the municipalities by defending their shared interests, helps to share knowledge and best practices, and provides services. VNG has founded a knowledge institution, *KING* (2017), to actively develop knowledge for municipalities. GEMMA for example, the reference architecture, is developed by KING.

5.4 Summary

Many different stakeholders are involved in the execution of the Dutch health care system. It depends on the act which stakeholders are involved. The ZVW covers all general health care. Health care insurers provide insurances covering a regulated set of health care, among which are medical equipment needed short term. Medical mobility solutions like mobility scooters are covered by the WMO which is executed by municipalities. A third act, the WLZ, covers long-term health care for chronically ill. Personal medical equipment needed in long-term health institutions is covered by the WLZ. Organizations that provide services like delivering medical equipment have to deal with the multiple stakeholders active in the different acts. This makes working in this industry rather complex. Another complicating factor is that the social health care system is always a subject of change. Which health care should be covered by which act for example is an ongoing debate.

6 Proposed solution approach

Based on the literature study covered in the previous chapters we can further analyze the problem as introduced earlier. This chapter will first of all cover this analysis and show the essence of the problem we try to solve. Next, based on the identified problem we will introduce the objectives for a possible solution. This solution, a methodology, will also be introduced in this chapter. The goal of this methodology will be to identify risks related to the processing and collecting of personal information and to mitigate this risks. A model of an organization's enterprise architecture can be used to analyze this risk and select suitable counter measures.

6.1 Problem analysis

The first element of the problem is the specific domain of the problem, the Dutch health care industry. The Dutch health care system is a unique system mainly regulated by a set of four laws. These four laws regulate the financing of many medical procedures, equipment and so on. Which health care acts is applicable depends on the kind of treatment, therapy or medical equipment needed. Each act has a different executive organization and other involved stakeholders.

Organizations operating in the health care industry have to deal with the different acts and as a result with the different stakeholders. A good understanding of these regulations is critical for their core business. Since the social health care system is subject of change due to changing political influence and new insights these organizations must be somehow constantly update their processes to match the new rules and regulations.

However, the most important motivation for this research are the challenges in relation to the privacy rules and regulations. Privacy is about having control over your personal information. To protect the privacy of individuals it is necessary to have rules and regulations. In the Netherlands the protection of personal information is protected by the (*Wet bescherming persoonsgegevens* 2000). A European directive that will soon be active in all countries of the European Union will unify the rules and regulation regarding privacy in these countries. The current and future privacy rules and regulations all limit the collecting and processing of personal regulations.

This is where the topics regulatory compliance and risk management become interesting. Regulatory compliance is about meeting restrictions that rules, regulations or agreements

Regulatory compliance and risk management are two field of interest that are heavily connected. Not being compliant often exposes some kind of risk. Or the other way around: being compliant with rules, regulations, standards and agreements reduces risks. As defined by (Racz et al., 2010) a holistic approach of risk management together with regulatory compliance and a third concept, governance, (GRC) will help to become more efficient and effective as an organization. An integrated approach is therefore preferred.

We now have a clear view of the domain under investigation, the Dutch health care sector, and better understanding of the challenges that come with privacy regulations. Being regulatory compliant with these regulations and thereby mitigating risks associated with not being compliant should be the primary objective to tackle this challenge. An integrated GRC approach may be part of the solution, but where to begin?

Risk management is about identifying, assessing and prioritizing risks. But before you can start identifying risks you need to establish the context. An enterprise architecture model seems to be a good starting point for the establishment of the context. An enterprise architecture is a blueprint of an organization. It typically covers both business and technology assets. With an enterprise architecture model you can visualize the 'as-is' situation of the organization.

There are already methodologies available that bring together risk management and enterprise architecture principles. In enterprise risk management the benefits of incorporating enterprise architecture are already acknowledged. One particular interesting methodology is the one designed by (Jonkers, 2014). The core of this methodology is a cycle which supports the identification and mitigation of risks. Each step in the cycle van be illustrated with an enterprise architecture view.

Can a methodology based on the existing methodology by Jonkers (2014) also be used to help organizations to comply with privacy rules and regulations? Is this methodology suitable to identify risks associated with the processing of personal information? Does a risk assessment together with enterprise architecture principles help organizations in the Dutch health care system to comply with privacy regulations while still being able to operate in the Dutch health care system?

The remainder of this paper will focus on these questions. A solution based on the mentioned methodology will be proposed, demonstrated, evaluated and discussed. The goal of the this design process is to work towards a generic enterprise architecture, a reference architecture. Such a reference architecture can be used by everybody in a certain domain, in this case the Dutch health care industry. It should support the design or redesign of enterprise architectures

and lay some groundwork to help these organization to become compliance with privacy regulations.

6.2 Enterprise architecture development

TOGAF's ADM is will be used to develop an enterprise architecture. As discussed in the literature is TOGAF a well-known and often applied framework in practice. The discussed reference architectures are based on TOGAF principles. Another reason to use TOGAF is the existing mapping between ArchiMate and TOGAF's ADM. ArchiMate is a powerful modelling language to visualize enterprise architectures. As discussed in the next section there is also a mapping between risk and security concepts and ArchiMate, one more reason to use ArchiMate and TOGAF.

6.2.1 Domain

An important motivation for this research is the specific domain in which the research is conducted. This domain is part of the context in which the enterprise architecture is developed. Eventually, elements of this enterprise architecture that are domain specific but not organization specific can be used for a reference architecture.

The domain specific architectural elements can be illustrated by different views. First of all, the actor co-operation view will be used to illustrate the different sales channels that are a result of the different social health care acts. This view helps to understand how the external business actors are related. A more detailed description of the external business actors has to be given to explain their responsibilities.

An organizational view helps to illustrate the different internal actors that are active, in which divisions they are active and help to identify the different responsibilities. Together with a description per internal actor this view should give a good illustration of the organizational structure.

A simplified high level business process cooperation view will be used to illustrate the main business process that is under investigation. The different business processes are broken down to a level where they can be linked to a single internal business actor.

6.3 Privacy risks and personal information management

For the execution of the privacy risk assessment we will follow a predefined methodology. This methodology will be based on an existing methodology and adapted for out use case. We choose to base the methodology on the methodology as defined by Jonkers and Quartel (2016). This methodology follows the common formula as identified by Ionita (2013): establishment of the context, the risk identification, the risk analysis, the risk evaluation and finally the selecting of counter measures. The Enterprise Risk and Security Management (ERSM) methodology as the methodology is called is shown in (Fig. 6.1).

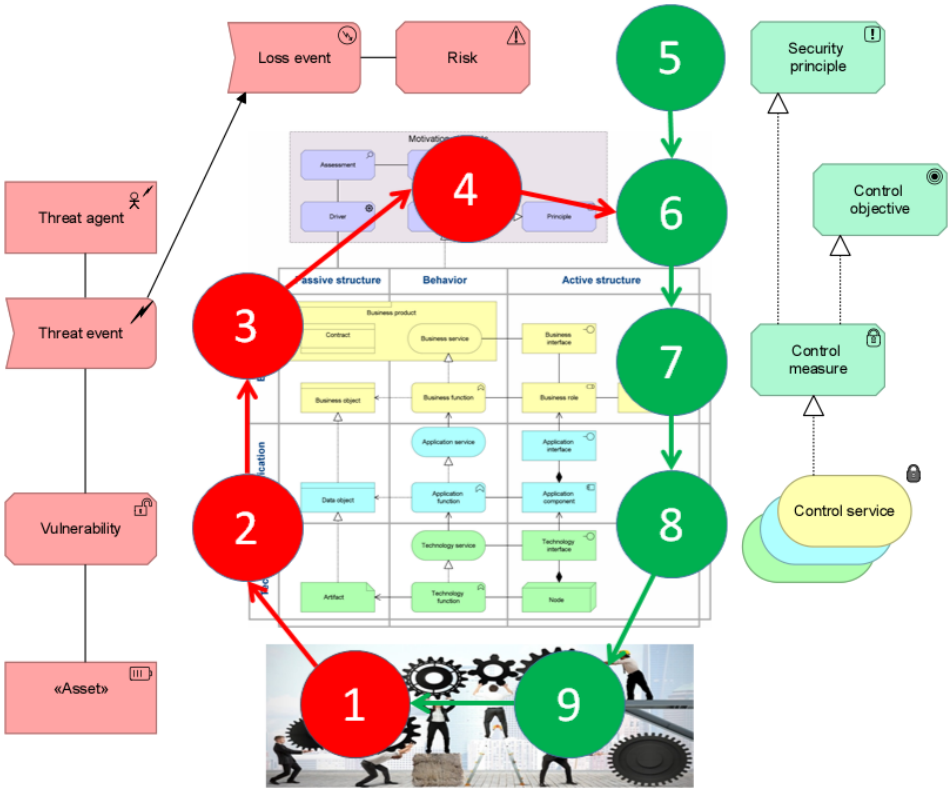

Fig. 6.1: BiZZdesign (2017) - ERSM Cycle

The methodology consists of 9 consecutive steps and is circular which means the output of the last step can be the input for the first step. The execution of the method can therefore iterative to support a continues execution of the assessment. The steps are divided into two phases. The first phase covers the risk assessment. The context is established (step 1), the risks are identified (step 2), the risks are analyzed (step 3) and the risks are evaluated (step 4). The activities in the second phase cover the selecting of suitable counter measures. The selecting of counter measures is divided into five steps leading to a well-founded selection of control measures.

Band et al. (2015) described the mapping of the risk concepts onto the ArchiMate core so these concepts can be modelled in architecture views. Jonkers and Quartel (2016) linked the risk

concepts to the steps of their proposed risk assessment process. During the first step the assets are identified, during the second step the vulnerabilities and so on. The complete mapping is shown together with the steps in (Fig. 6.1). This means that every step can be supported by a view modelled in ArchiMate. This mapping will be used to illustrate the executed steps.

The remainder of this section will focus on how these steps will be executed. Jonkers and Quartel (2016) don't specify specific views or methods on how to execute the steps. For every step a description will be given on how we propose to execute these steps and with which architecture views the steps can be illustrated.

Besides, our methodology will focus on privacy and the risks associated with collecting and processing personal information. This will influence the interpretation of the steps.

6.3.1 Step 1: Monitoring

The monitoring of the operations under investigation results in a baseline architecture covering a certain part of the organization. The assets modelled in this step will be under investigation during this assessment. The result is a view on the enterprise architecture covering the scope as defined earlier.

To keep this monitoring step structured and clear the proposed view only covers a single detailed business process. When multiple business processes are covered by the scope of the assessment each should be presented in a separate view. The business process is at the center of the view. Linked to the business process the associated business actors, business objects and application services are modelled.

6.3.2 Step 2: Vulnerabilities

The identification of the vulnerabilities will be done based on conversations with information manager at Welzorg and based on an existing list with common vulnerabilities (Kosutic, 2017). By using these methods both the specific vulnerabilities for Welzorg as well as the vulnerabilities that generally occur in organizations are covered. Combined, these methods will probably give enough information about the possible vulnerabilities that currently are a major issue and can lead to a threat.

All identified vulnerabilities should be related to assets in the enterprise architecture. It is the asset that exposes the vulnerability. Therefore the vulnerabilities are illustrated in the same view as the assets that are identified in the previous step.

6.3.3 Step 3: Threats

To illustrate how these vulnerabilities can be misused and exploited the possible threats should be identified. Threats can be initiated by threat agents who can as well be modelled in the architecture.

Vulnerabilities can be misused in different ways leading to different threats. This also depends on the threat agent and the intentions of this agent. Not all threat agents are hostile and try to do harm. An example of a non-hostile threat agent is a reckless or untrained employee who unintentionally does harm by his actions. But most threat agents that typically can be identified are hostile an intent to do some kind of harm. Examples are vandals, competitors or activists (Casey, 2007). By taking some of these threat agents as an example it is easier to identify how the vulnerabilities can become threats.

For this step we choose to only identify a single threat per vulnerability. This is done purely to demonstrate how the vulnerabilities can be misused. This list will not be all-encompassing. First of all because different threat agents will expose different threats and secondly because a vulnerability can often be misused in different ways and therefore expose different threats.

To illustrate these threats a view is proposed where only the vulnerabilities linked with an example threat are mapped. This view gives a clear illustration of how the vulnerabilities as identified earlier can become a threat. Such a view emphasizes the importance of these vulnerabilities.

6.3.4 Step 4: Risks

Eventually the threats can lead to loss events, an actual loss of control over an asset or a loss of the asset itself. The impact of a loss and the frequency of a possible loss event together result in the actual risk. The actual loss events will not be identified. A loss event is an actual occurrence of a threat. The appointing of these loss events during this analysis doesn't give much more insight.

The focus will be on the risks for the organization: only the risks for the organization under investigation will be identified. The motivation to mitigate these risks will be biggest since possible losses will be at cost of the investigated organization. This approach makes the exposed risks tangible and shows the impact that having the identified vulnerabilities could have.

By not indicating how loss events can occur a qualitative analysis becomes hard. A qualitative risk analysis uses qualitative measures to eventually identify the level of risk. Risks can then be qualified for example as low, medium, high or critical based on the frequency of a loss event and a level of vulnerability.

6.3.5 Step 5: Security policy and principles

The first step of the second phase, the security deployment phase, isn't actually in the cycle. The definition of policies and principles representing the organization's risks appetite can be done independently of a risk assessment. In TOGAF ADM these principles are actually designed in phase A and should be update when necessary. But when these principles and policies are designed and there is no need to update them they can be used for each risk assessment executed within the organization.

Since the focus during this assessment is on privacy we should try to capture the privacy related policies and principles. An important guideline for privacy are of course the privacy rules and regulations. Most organizations will have a basic principle stating the organization will comply to local rules and regulations. This means they will also try to comply to the privacy rules and regulations. But this is still a bit vague. What does this mean for the organization? Maybe it is possible to capture the requirements that are a result of the wish to comply with the privacy regulations in enterprise architecture elements.

The policy and principle concepts seem to fit the requirements that are a result of the privacy regulations. Policies are concrete implementations of principles. Policies can therefore be used to present a concrete representation of the articles that make the privacy acts. The mapping to ArchiMate elements and therefore the representation of the privacy regulations in a view is now a small step. Principles can already be represented by an element in the motivation extension of ArchiMate. Policies are represented as security principles as proposed by Band et al. (2015). The result of this step will be a view capturing the requirements of the privacy regulations represented as principles and policies.

6.3.6 Step 6: Control objectives

Based on the risks that should be mitigated and the security policies and principles the control objectives are formulated. They guide the selection of requirements for control objectives in the next step. The control objectives are high-level security requirements designed to mitigate the risk.

There are some common used lists with control objectives. Security management standard ISO/IEC 27001 (2013) covers a list of security objectives based on best practices. These are general objectives that can help organizations to effectively achieve information security. The objectives are designed to achieve general information security. The processing of personal information will also benefit from the implementation of these objectives since the personal information is a subset of all information processed by an organization.

Trying to comply to all control objectives as proposed by ISO 27001 at once isn't reasonable since there are too many and more importantly they don't all relate to the risk we try to mitigate. Therefore, a selection has to be made based on the identified risks and policies.

6.3.7 Step 7: Control measures requirements

The requirements for control measures are specific requirements and a low-level interpretation of the control objectives. These requirements are selected based on the control objectives and are linked to the identified vulnerabilities. The requirements for the control measures are however still high level and not a detailed description of the proposed solution.

During this step the control objectives and the vulnerabilities come together. The control measures clearly reduce the weakness that is represented by the vulnerability and implements the control objective. The proposed view to illustrate this is a view covering the vulnerabilities, the control objectives and the control measures.

6.3.8 Step 8: Control measures design

This step should result in the design of one ore more actual measures that meet the requirements. The control measures can be modelled with elements in the enterprise architecture in any layer meaning the solution can be a new procedure (business), adjustment of application services or have impact on the technology.

For the purpose of this assessment we will not design every control measure as proposed. We will just give an example of how control objectives can be designed. The illustrated solution will not be the only way to implement the control measure. There isn't only one design possible that implements the control measure. The design will differ from organization to organization to fit in the existing architecture.

6.3.9 Step 9: Operational control measures

Finally the designed solution(s) should be implemented which leads to a new baseline architecture with operational control measures. The actual implementation of the control measures is out of scope of this research and therefore not be covered by this methodology.

6.4 Summary

A full approach is given for the analysis of privacy related risks and the selection of counter measures to reduce the risks. First of all we try to capture the characteristics of the domain. Architectural views covering internal business actors, external business actors and the main sales channels together with short deceptions should give a high level view of the industry and the organization under investigation. These views should give some understanding about the challenges that come with the specific domain.

For the analysis of the risks related to the collecting and processing of personal information we have developed a methodology based on an enterprise risk and security management methodology. The privacy and personal information management methodology is the developed tool to do so. The methodology consists of 9 steps of which 8 are described in detail. The steps have to be executed consecutively. The detailed descriptions of the steps cover how the steps should be executed and how the result should be communicated. An important part of the communication are the enterprise architecture views modelled in ArchiMate. Tab. 6.1 summarizes the steps together with the literature or inputs that is used to formalize the steps and a reference to the ArchiMate view used to illustrate the output of the step.

No.	Step	Input	View
1	Monitoring	Interviews and Documentation	Fig. 6.2 A
2	Vulnerabilities	Kosutic (2017)	-
3	Threats	Casey (2007)	Fig. 6.2 B
4	Risks		Fig. 6.2 C
5	Policies & Principles	*Wet bescherming persoonsgegevens* (2000)	Fig. 6.2 D
6	Control objectives	ISO/IEC 27001 (2013)	-
7	Control measure requirements	Control objectives and Vulnerabilities	Fig. 6.2 E
8	Control measure		-

Tab. 6.1: Step by step

The designed artifact is supported by literature but has to be validated. In the next chapter the methodology will be applied on a set business processes at a selected organization. With this case study we will try to validate the designed methodology and identify possible shortcomings.

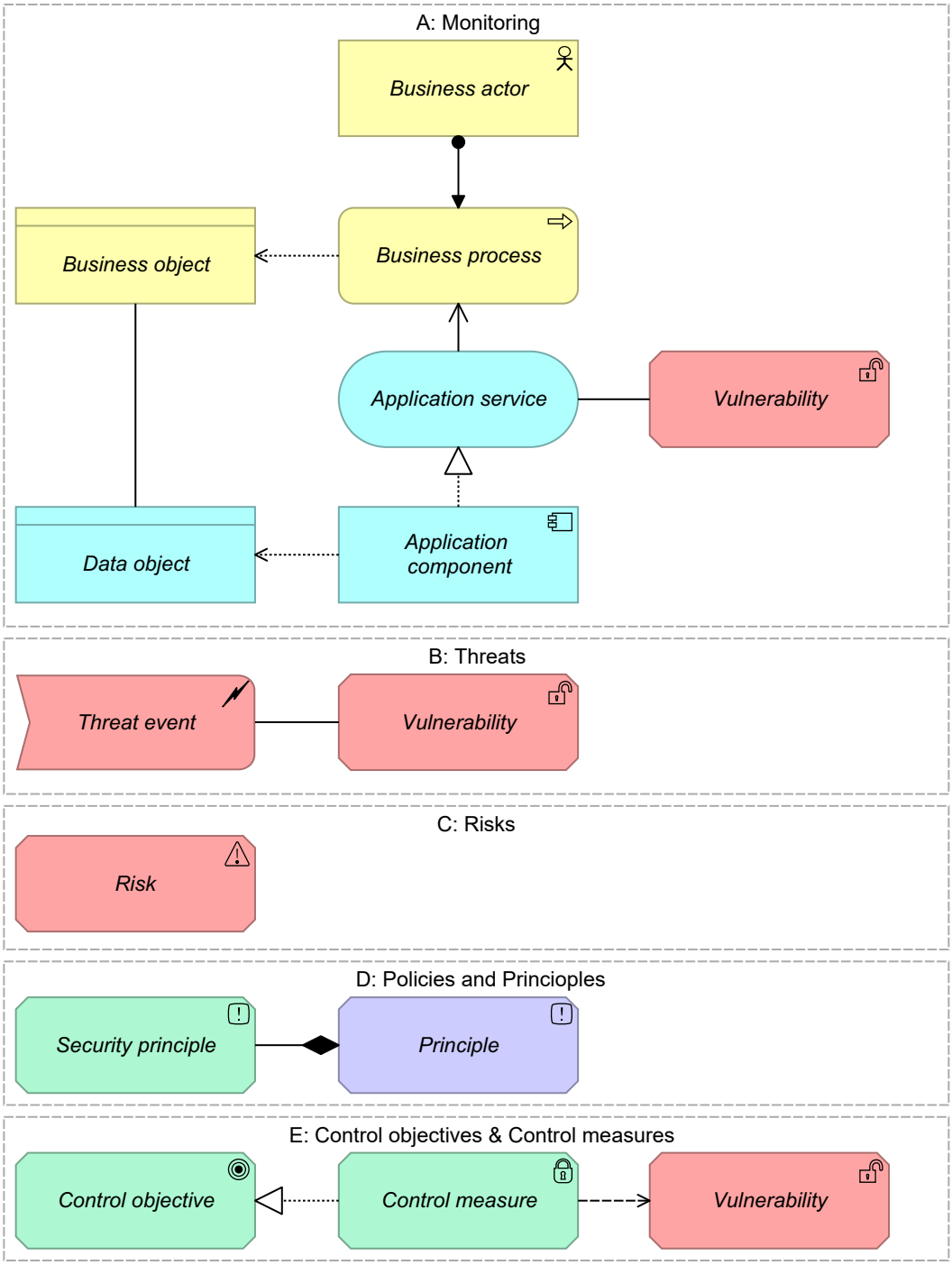

Fig. 6.2: ArchiMate architecture views

7 Case Study at Welzorg

7.1 Baseline Enterprise Architecture Welzorg

The baseline enterprise architecture shows the current, or 'as-is', enterprise architecture of an organization. In this chapter the internal and external actors are introduced as well as how they are related to each other. The relations between external actors depends on the covered sales channel.

7.1.1 External Business Actors and Roles

Client

The client is the person in need of a medical supply. This can be due to a temporary injury, declining mobility related to for example age or long term illness due to chronic illness. Depending on the background for the need the client has the right to get a medical supply based on the WMO, WLZ, ZVW or has to pay for the supply himself. Sometimes clients have the right to get medical supplies based on multiple acts. Depending on the act that is executed, the client has to deal with either his municipality, his health insurance company, the health office or health-care facility, or directly with a medical supply company.

Municipality

A municipality is responsible for the execution of the WMO for his citizen. Municipalities are obligated tot provide medical supplies for the citizens in need. They do so by contracting one or multiple organizations that can provide these medical supplies covered by WMO. The municipality is the first contact point for citizens in need for medical supplies. The municipalities will instruct a contracted medical supply provider after an interview with the client to deliver an suitable medical supply. The municipality manages the budget and audits and pays the invoices submitted by the supplies organizations.

Health Insurance Company

Dutch citizens are obligated to have a basic health insurance. These insurances are provided by private health insurance companies. This basis health insurance also covers some cases where

medical supplies are provided. Typically, these are cases where the need for a medical supply is temporarily. For example, when a client breaks a leg and is in need for crutches. This is called short term lease (Dutch: kort durende uitleen, KDU). In these cases the client can look for an appropriate medical supply provider and order the needed. Health insurance companies have contracts with many health providers, including medical supply providers. When this is the case, the medical supply provider can send the invoice directly to the health insurance company of the client.

Long term health facility

A Dutch long term health facility or nursing home is a facility financed by the WLZ. The facilities that are WLZ approved are the home of clients that need a lot of care for a long time, often chronic. The facilities are specialized in a specific type of heath care. There are nursing homes for the elderly, homes for clients with dementia or Alzheimer's, homes for clients with a psychological disorder and so on. In some of these facilities there is also a need for personal medical supplies. These medical supplies are for example: electric wheelchairs equipped for one person, wheelchair with orthotics and bed boxes.

Health office

The health offices plays a central role in the execution of the WLZ. The health offices are region bound and are the first contact point for clients that are entitled to WLZ health care. In the Netherlands there are 31 regional health offices. Each office is operated by a health insurer that has historical biding with the region. One of the possible prescriptions is a stay in a long term health facility. The health offices deal with the invoices and financing of the WLZ.

Medical Supply Provider

The crutches, scooters, wheelchair and other health care products as mentioned earlier are provided by medical supply providers. These organizations get their delivery and service orders through multiple channels. When contracted by a municipality they have to provide medical equipment for the citizens of these municipalities. Once a municipality assigns a type of equipment to a citizen the entire process for delivering an servicing is handed over to the medical supply provider. The core processes of medical supply providers typically cover the assessment of requests for medical equipment, the selecting of the medical equipment, the delivery, repair services and finally return handling of the equipment. In the next section the multiple order channels are explained in more detail.

7.1.2 Sales Channels

Depending on the health care act that is executed different actors are active and work together to provide the medical supplies for the client. In the following section the different views are presented for each act an how the actors together realize the business processes.

WLZ

In order to qualify for WLZ health care a client needs to get a health care assessment. Once a client has an assessment he can go to his local health care office to get the care he needs. One of the options is to get treatment in a WLZ facility. Sometimes a client in a facility needs specially adjusted equipment which are ordered at medical supply providers. The health offices do the financial handling. The real situation is actually a bit more complex but for now simplified to what described above. From Welzorg's point of view this description is sufficient. The institutions order their equipment at Welzorg and Welzorg sends the invoices tot the health offices. The invoice procedure depends on the health insurer operating the health office.

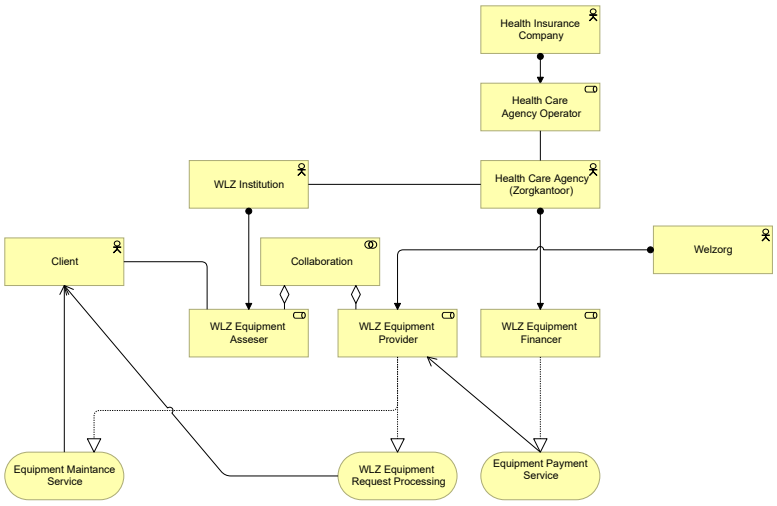

Fig. 7.1: Actor Co-operation view WLZ

WMO

The WMO is the most important sales channel for Welzorg. The WMO is executed by the Dutch municipalities. They contract organizations like Welzorg for the medical equipment and solutions that are covered by the WMO. The contracts are publicly tendered and offers are rated based on the public available assessment criteria. The contracts are not standardized and every municipality has his own set of assessment criteria. Thus Welzorg has a portfolio with different kind of contract containing different terms and conditions.

The biggest variable in the contract is whether a contract based on a 'buy' or a 'lease' concept. With a 'buy' contract the municipality becomes owner of the medical equipment. These kind of contracts often come with a limitation in brand or type of equipment that should be provided. This equipment is not always part of the core assortment of Welzorg. With a 'lease' contract Welzorg is the owner of the equipment. Welzorg has more freedom in these contracts to choose the proper equipment. The contract also regulates the maintenance and repair service and covers a service level agreement.

A citizen in need of medical equipment can request for one at his municipality. The municipality will review the application and when approved send the application to a contracted equipment provider. The medical equipment provider will take it from there and invoice the municipality for the delivered services.

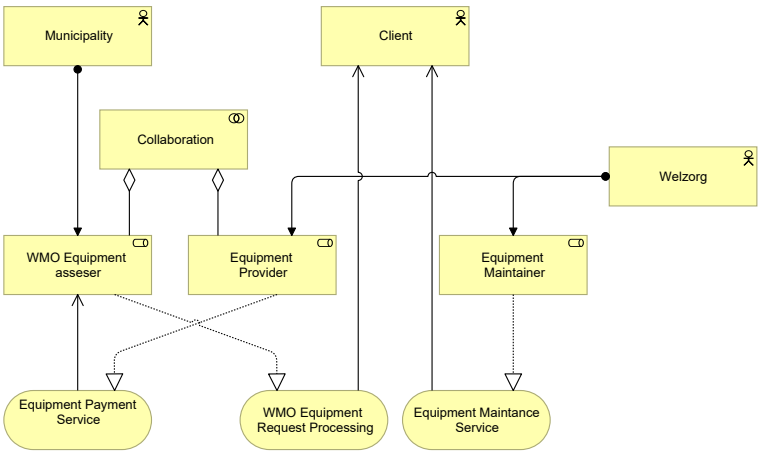

Fig. 7.2: Actor Co-operation view WMO

ZVW

Every Dutch citizen has a health care insurance at an insurance company. The insurance companies have contracts with all kind of health care providers to deliver care for their clients, with the health supply providers for example. The ministry of health decides which services are covered by the ZVW but clients can decide to take an addition insurance covering more than the basic services. With a referral for medical equipment covered by the client's insurance the client can request the medical equipment at Welzorg. With the information provided by the client Welzorg can, when the health insurer is contracted, send the invoice directly to the health insurer.

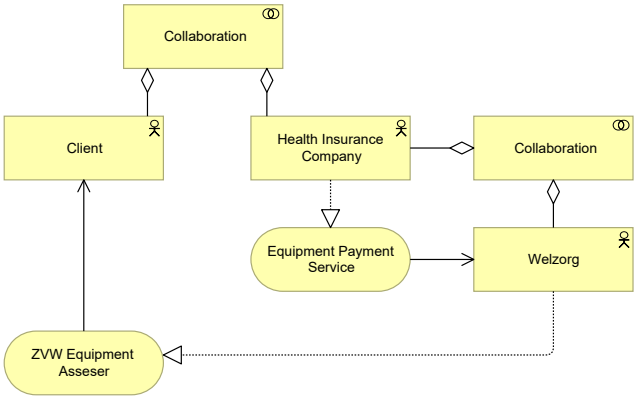

Fig. 7.3: Actor Co-operation view ZVW

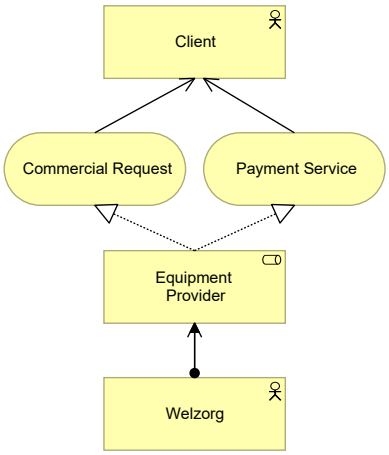

Fig. 7.4: Actor Cooperation View Private Sales

Private Sales

Sometimes the medical equipment isn't covered by one of the above acts or sometimes people choose to buy their own medical equipment. This fourth sales channel is also available at Welzorg. Client can buy medical equipment at stores or at the web shop.

7.1.3 Internal Organization

The internal organization of Welzorg is outlined in the organization structure view. In this nested view, the division of Welzorg and the sub divisions are shown that are involved in the main process (Fig. 7.5). In the following paragraphs the roles of the divisions are further explained.

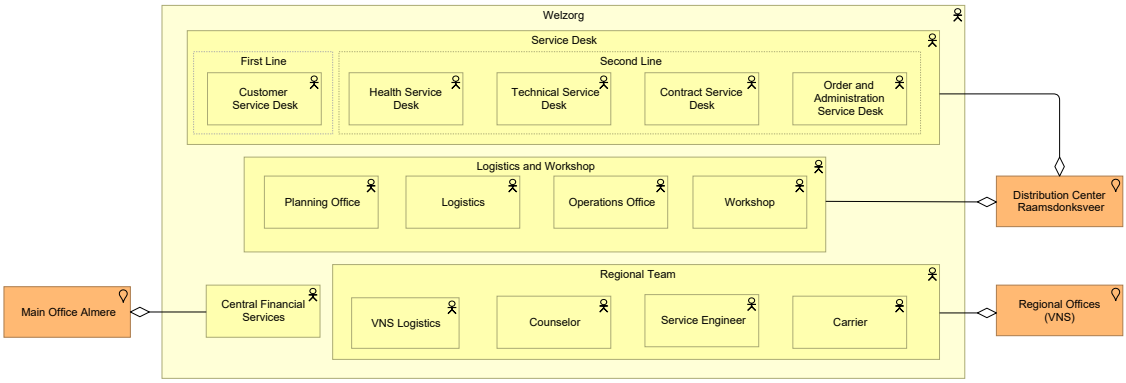

Fig. 7.5: Welzorg Organizational View

Service Desk

First of all there is the service desk division. This division consists of multiple sub divisions, the biggest one begin the *customer service desk* also called the first line service desk. This division handles the initial and general contact with clients. They answer questions, do simple consultations, plan deliveries and intakes.

The other service desk sub divisions are second line service desks. The *health service desk* do more complex consultations. Some health care specialist work at this division that are able to assess client's needs regarding medical equipment. The *technical service desk* can answer questions about the equipment and components used. The *contract service desk* has a great knowledge of the different contracts with municipalities, health insurers and health institutions. Finally, the *order and administration service desk* are specialized in answering questions about invoices.

Logistics and Workshop

The logistics and workshop division includes many operational processes which are executed in the main distribution center. This division consists of several sub division. The *planning office* is responsible for the planning of resources. The *operations office* division operates the warehouse, they select the equipment based on the requirements they receive. When there isn't any equipment in store they will order new equipment.

The *logistics* team will pick the orders and prepare equipment for transportation. Sometimes small adjustments are needed to make the medical equipment fit the client's needs. This is done by the *workshop* division.

Regional Offices

Welzorg has about 20 local offices called VNS's (Dutch: Vestiging Nieuwe Stijl). These offices function as a hub for the region they are in. The regional offices are supplied by the logistics department. A *logistics* team at the regional office handle the incoming equipment. *Carriers* carry the medical equipment to the client. *Service engineers* operate from the regional offices and do reparations at clients home. Finally the health *counselors* have the regional offices as their main office. They visit (new) clients at their home, rate their needs for medical equipment and request the appropriate needs.

General divisions

There are multiple general divisions, but the scope of this research covers only one. The *financial services division* is responsible for the final billing and administrative processing. This division ensures all documents are in order and sends the bill to those who should pay. Every different sales channel has a different procedure.

Outsourced Services

Welzorg has outsourced one division. The transportation from the distribution center tot the regional offices is done by an external company. The transportation takes place at night to shorten the delivery time to the customer. The carrier picks up all equipment at the DC and delivers them to the regional office.

7.1.4 Basic Request Handling

The scope is limited to the basic request handling. The basic request handling is the processes which starts with the request for medical equipment and ends with the processing of the payment. In between some processes take place which will be described in this section. The scope is further limited to WMO requests, this means the request will always start with an request by a municipality or is commissioned by a municipality. The processes will not differ much for the other sales channels, the main changes will be the applicant and the party that is billed.

The chosen level of detail gives a broad overview of the different process steps that are carried out. More detail would make this overview unclear. The request handling is also reduces to its core, leaving out many exceptions and alternative flows. The basic request handling focuses on the requests that can be fulfilled by equipment from the core assortment, where the requirements are clear an no further approval or reviews by trained staff is needed. More complex request require additional steps or the involvement of specialized internal actors.

However, this basic request handling process covers most of the requests and therefore covers many operations executed by Welzorg.

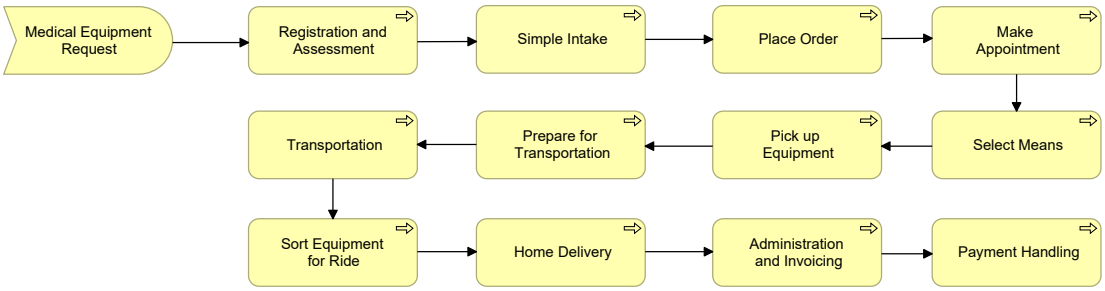

Fig. 7.6: Basic Request Handling

The initial request can be submitted through different channels. One of the main channels is through the WMO portal. This is a Welzorg website used by many municipalities to apply new medical equipment for their citizens. A second channel is the application by e-mail.

First of all the client needs to be registered. Some personal information is stored together with the initial request. This information is provided by the requester. In case of a WMO request this is the municipality. Based on the provided information Welzorg decides what kind of further action is needed. A customer support employee will assess the request and decide whether more information is needed or whether the processing of the request can continue. A main selection criteria is the type of equipment and whether there is more information needed from the client to select a proper solution.

The choice of equipment isn't only determined by requirements based on the assessment but also by contractual agreements. The contract can for example prescribes a certain brand or prescribes certain procedures. When the customer service desk employee has assessed the request an has all information to continue the request he will continue with selecting the proper equipment requirements and place an order with the requirement. Finally the customer service desk will make a delivery appointment with the client.

The next step in the basic request handling process is carried out by the operations office. They will select the actual medical equipment from stock and make a pick order. An order picker will actually pick the equipment from stock and prepare it for transportation. A delivery note and an user agreement will be attached to the equipment since they are needed later in the process. Sometimes some adjustments are needed to customize the equipment to the clients needs. These adjustments are carried out by the workshop department.

An external transportation company will transport all equipment for one region to a VNS. Here some logistics employees will select the equipment for each carrier based on the information on the delivery note and put it in their vans. The carrier will follow a given route based on the

appointments with the clients. The equipment is delivered and the client will have to sign the user agreement and confirm the delivery.

The signed user agreement is returned to the VNS and scanned. The financial department will do certain checks before sending a bill to the municipality. The delivery has to be taken place and a signed user agreement must be available. These conditions must be fulfilled, only now the municipality can be sure and check the request is carried out as agreed.

7.2 Privacy Risks Assessment

7.2.1 Monitoring

In this first step of the risk assessment we will monitoring the baseline architecture. This means we will in further detail describe the architecture in preparation of the next step of the risk assessment, the identification of vulnerabilities. We will analyze each separate step in the basic request handling process as described in the previous chapter (Fig. 7.6). The view will be limited to the business, data and application layer. The assets in the technology layer will not be included. The view will also include the associated vulnerabilities. In the next section the vulnerabilities will be further explained. Each separate process step of the basic request handling will be covered in this section and illustrated with detailed view.

Registration and Assessment

When a request for medical equipment arrives the information in this request needs to be registered. The request can arrive through several channels, for WMO requests this is likely the Welzorg WMO web portal or through email. The information can be separated into two business objects: the information regarding the client and information regarding the request. A more detailed view, but still high level, of the information regarding the client and the request is given in (Fig. 7.7).

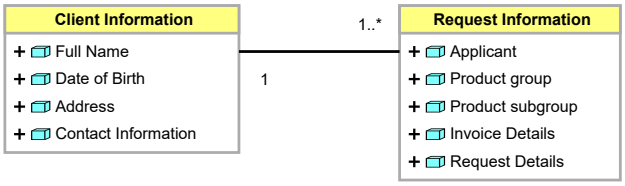

Fig. 7.7: Caption

When the information is processed and submitted in the service request management component the customer service desk has to assess the request. He will check whether the provided

information is complete and who should take further actions. When he rates the request as complete and 'simple' the next process executed will be the simple intake.

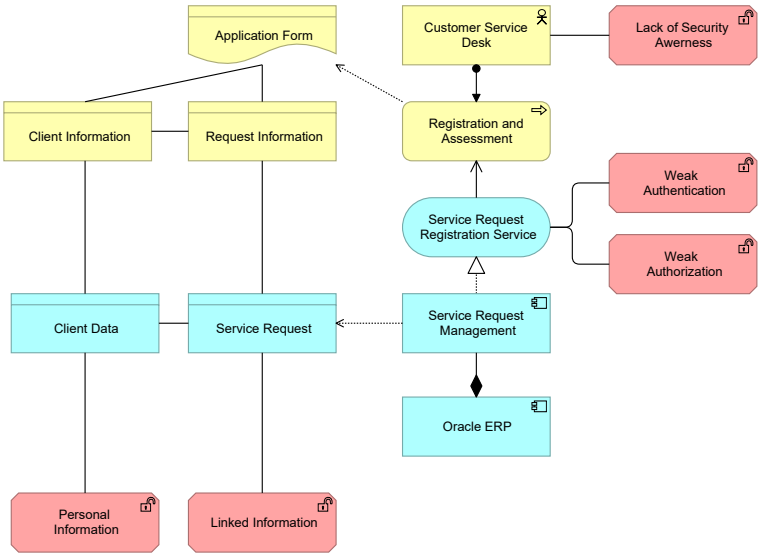

Fig. 7.8: Request Assessment

The service request management component is part of the Oracle ERP. After the execution of the process the result are two data objects containing the information regarding the request. Together these assets result in the model as presented in (Fig. 7.8).

Simple Intake

Although the name may suggest something different the simple intake process can be a complex step. The name simple intake is chosen since this step can be carried out by the customer service desk and doesn't need any other skills provided by for example the counselor or the health service desk. These other business actors can carry out more complex applications for medical equipment.

The complexity in the simple intake process is due to the high number of different contracts and sales channels. Although we have limited the scope of this assessment to WMO applications there are still many different agreements due to the different contracts with municipalities.

The simple intake is the process step where the available information is being examined which results in the requirements for the solution or the client. This process needs information about the original request and information about the contract to select the appropriate solution for the client. Sometimes additional information is needed which can be provided by the client over the phone. The request information is served form the service request management application component which is part of Oracle ERP. Information about the contract is stored

in the knowledge database. The result of this process is a service request with a detailed description of the required equipment by the client.

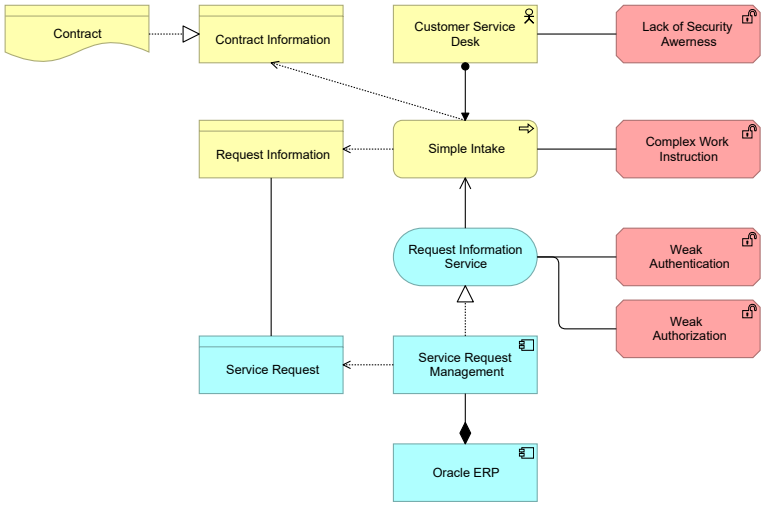

Fig. 7.9: Simple Intake

Place Order

Based on the information of the previous step an order can be placed. This activity is also carried out by the customer service desk. The order is linked to the service request and contains detailed information about which equipment is needed. Based on this information the operations office should be able to select the equipment needed.

Make Appointment

To make an appointment the customer service desk needs multiple peaces of information. First of all it needs the address of the client to know where to deliver and which carriers are active in the clients region. Together with the availability of the service operator the appointment can be scheduled. The appointment is made with the scheduling component of the Field Service Suite.

The appointment is linked to the client and to the equipment that needs to be delivered. This information is stored in the scheduling component. The storage of the personal information is a vulnerability. This makes the link tot the scheduled appointment a vulnerability. The information presented to the user, the customer service desk employee, by the agreement scheduling service. The access to this service is also a vulnerability.

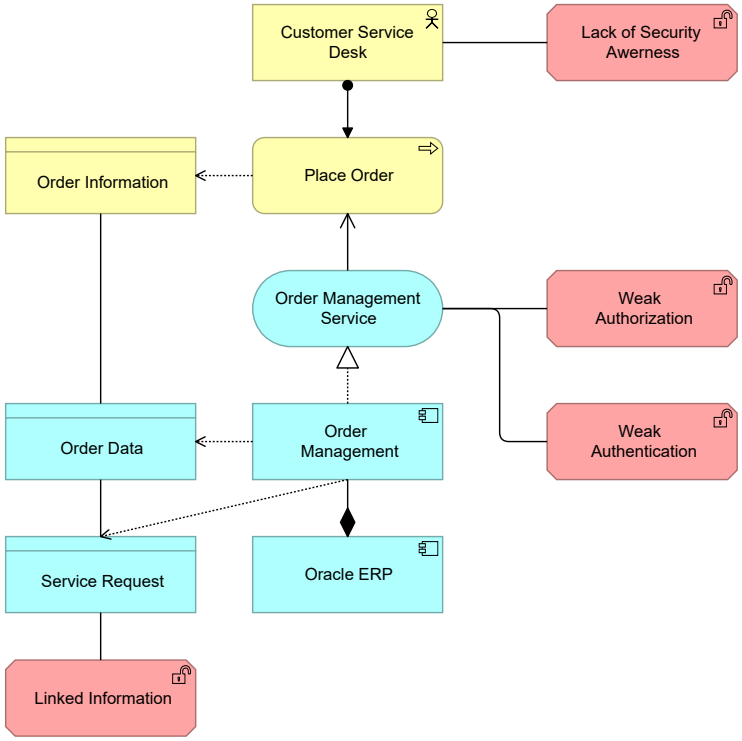

Fig. 7.10: Place Order

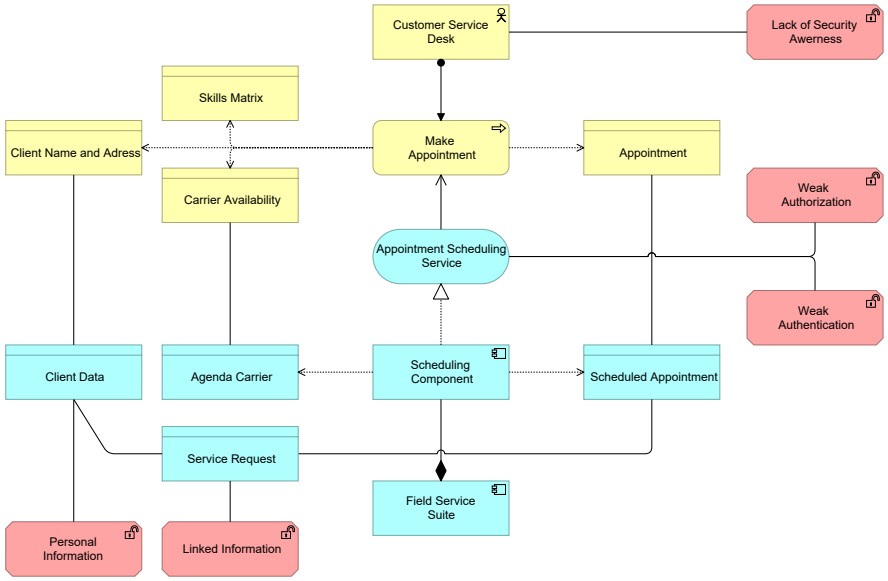

Fig. 7.11: Make Appointment

Select Means

Based on the information collected by the customer service desk the operations office can actually select the appropriate means from stock. For this step the operations office only needs the order information. This process will result in a picking order which will be carried out by the logistics team.

The inventory management application will provide information about the equipment available in stock and the properties of the equipment. The order management module contains the information collected by the customers service desk. Both modules are part of the Oracle ERP suite.

Pick Up Equipment

The logistics team carries out the pick-up orders compiled by the operations office. To execute this process limited information is needed. The logistics employee only needs information about which equipment should return, where it is located and where to drop it off.

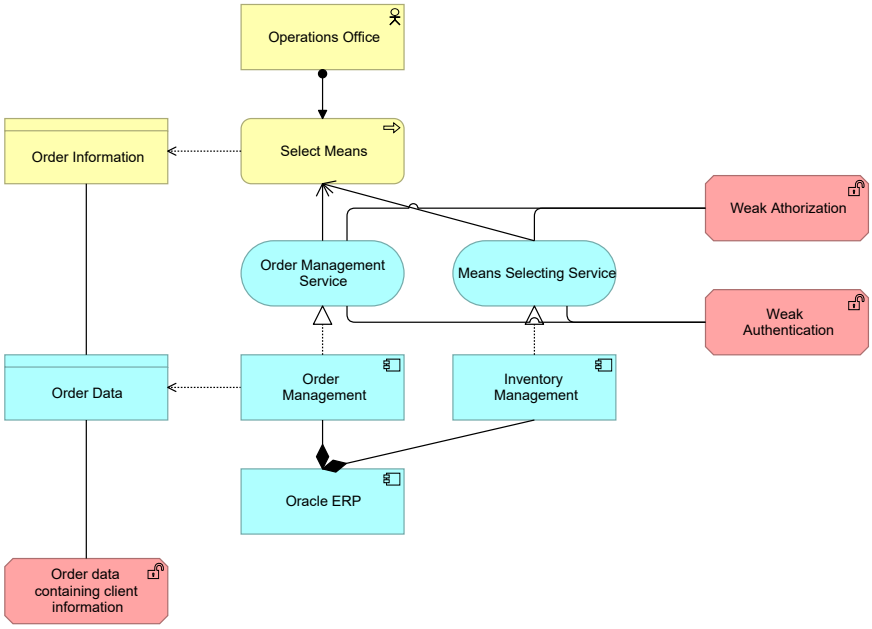

Fig. 7.12: Pick Up Equipment

Prepare for Transportation

The preparation for transportation is a process that actually includes several sub processes. Out of scope are the additional actions are sometimes needed when equipment needs to be adjusted. These actions carried out by the workshop are part of the more complex request handling process. First of all the printing of the user agreement. This is an agreement with

including some personal information that has to be signed by the client. Secondly, a delivery note is printed. This note includes some detailed information about the client and where the equipment should be delivered. Both documents are attached to the medical equipment. The final step is putting the equipment in the right dock for transportation.

To create both documents personal information is used, which should happen carefully. Besides this information is printed which exposes another vulnerability.

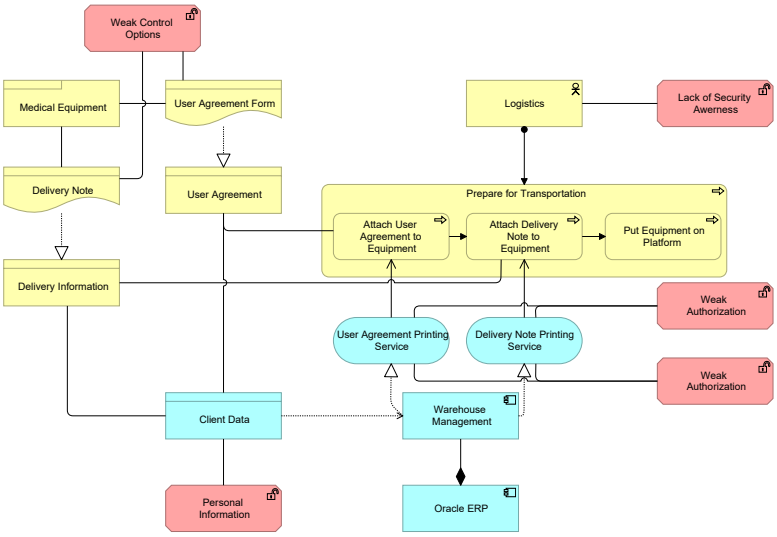

Fig. 7.13: Prepare for Transportation

Transportation

The transportation process is executed by a third party carrier. The carries takes the prepared equipment at night to the VNS's. The equipment is already collected at a specific dock at Raamsdonksveer. Remember the equipment has the notes attached, which can be a vulnerability.

Sort equipment for ride

Before the home delivery can take place the equipment as delivered at night by the transportation organization should be divided over the carriers. The VNS logistics team decides which equipment should be put in which van by looking at the delivery note as attached to the equipment.

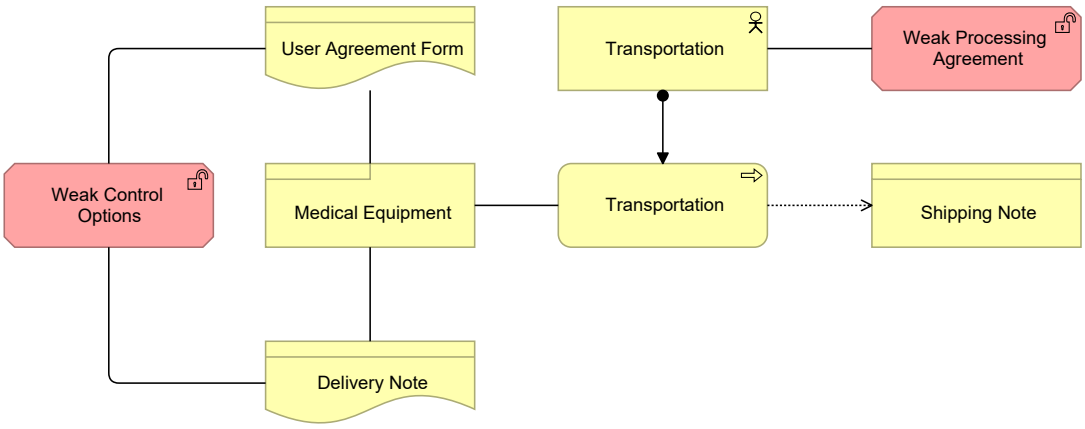

Fig. 7.14: Transportation

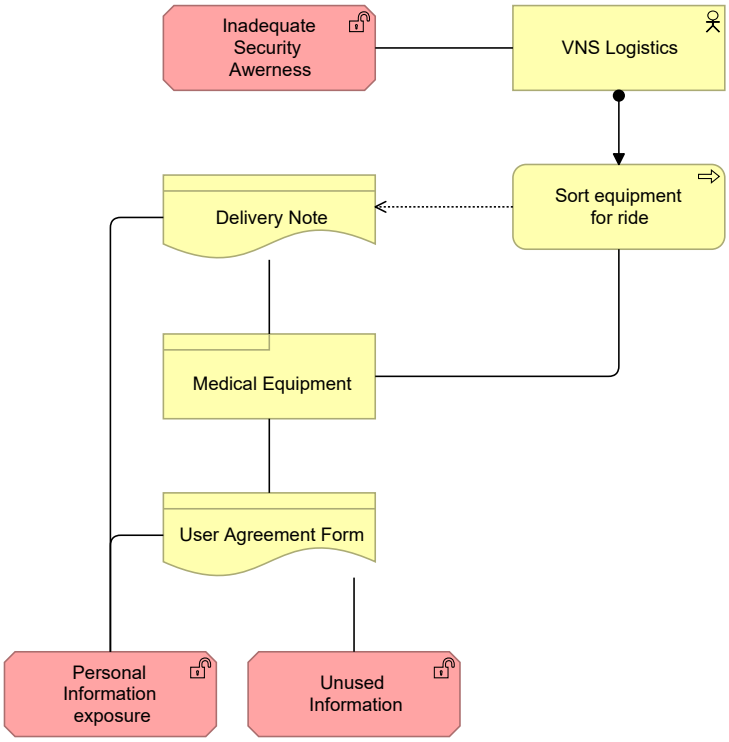

Fig. 7.15: Sort Equipment

Home delivery

The goal of all previous processes is off course the delivery of the equipment to the client. The carrier brings the equipment to the client. The client has to sign for it. The client also needs to sign a user agreement.

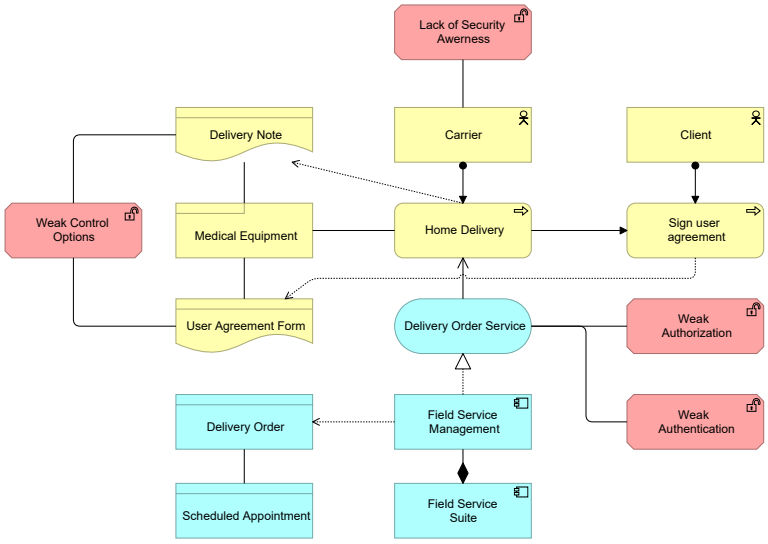

Fig. 7.16: Home Delivery

Administrative processing

The final process is the administrative processing. The financial department will send an invoice to the applicant. Before this can be done the central financial services department will do certain checks

7.2.2 Vulnerabilities

Vulnerabilities are weaknesses of assets in the organization. With the baseline enterprise architecture available we can scan it systematically for vulnerabilities. For every modelled asset we can evaluate whether they have a vulnerability or not and link it to the asset. The vulnerability assessment will focus on vulnerabilities that can affect privacy. Not all vulnerabilities are only linked to privacy, many vulnerabilities also compromise overall security.

One way to systematically identify vulnerabilities is the executing of a penetration test. The found vulnerabilities can be mapped to the monitored enterprise architecture. Vulnerabilities are often written down as weaknesses or a lack of something related to one of the assets. As can be seen in the previous step where the vulnerabilities are already visualized in the model

and linked to the assets to which they apply many vulnerabilities pup up in multiple processes. In this section the vulnerabilities are further investigated and analyzed.

Weak authentication

A user should identify himself through a solid authentication process. Having weak authentication means user could identify himself as someone else or there isn't even any identification needed to access systems. This makes the services vulnerable for unauthenticated access.

Weak authorization

Weak authorization is a vulnerability where users have access to assets which they don't need to perform their assigned tasks. This is a vulnerability where the more services than necessary are available for certain business users. This makes the services vulnerable for unauthorized access, even when the user has identified himself through a solid authentication process.

Lack of security awareness

Employees with a lack of security awareness is a vulnerability. By not executing the company security policies the employee exposes a vulnerability. The reason can be carelessness or malice by doing it on purpose by deliberately ignoring the guidelines, or by the lack of policy awareness. Either way the lack of awareness exposes a clear vulnerability with the possibility of losing personal information.

Wrong execution of work instructions

Complex tasks are vulnerable for misinterpretation or being wrongly executed. This vulnerability is related to processes that come with extensive work instructions. Mistakes are easily made during these processes and when working with personal information this can far-reaching consequences. When personal information is stored on the wrong location due to wrongdoing for example control over this information is lost.

Weak control options

The control over physical assets is difficult. Especially the control over forms which can be a problem when these forms contain personal information. Authentication and authorizations options are limited when dealing with physical forms. Therefore the vulnerability linked to physical forms containing personal information is the weak control options.

Weak processing agreement

The involvement of an external third party business actor during the execution of processes exposes some unique vulnerabilities. When dealing with a external actor there should be special attention for the information shared with this actor. Since the processing of the information by the partner isn't under direct supervision there should be some agreements between the two parties to ensure some level of security. Besides the responsibility of sharing only the required information there should be a processing agreement covering the information that is shared. A weakness in this processing agreement exposes a vulnerability.

Personal information

By defining the presence of personal information as a vulnerability it is easier to to identify which related assets need to be further investigated. These assets will somehow process or access the personal information and the vulnerabilities of these assets will have effect on the privacy. Processing personal information is therefore by definition a vulnerable activity.

Linked information

By linking information the information itself becomes more valuable. This makes linking information a vulnerability, especially in combination with the presence of personal information. Linking information assets creates value through synergy. Awareness of this effect is important since the risk related to the single information assets may be low, but for the assets together the risk may be substantially higher. This is why linked information is identified as a vulnerability.

The vulnerabilities covered in this analysis don't go deeper than the data layer. The possible vulnerabilities in the technological layer are not taken into account. There are many tools available to execute penetration tests, especially on the technological layer. The typical vulnerabilities in this layer are not specifically related to privacy. This makes this layer less interesting for the analysis currently executed. And overall security assessment will cover these vulnerabilities.

7.2.3 Threats

The vulnerabilities as identified above can be used by threat agents to damage or otherwise compromise the associated assets and therefore form a threat. Using a threats is the exploiting of vulnerabilities to cause harm. The threats can be manifested by threat agents. These threat agent can be anyone, these can be organized crime or criminals, activists or even your own employees.

Almost every vulnerability can be exploited and therefore become a threat.

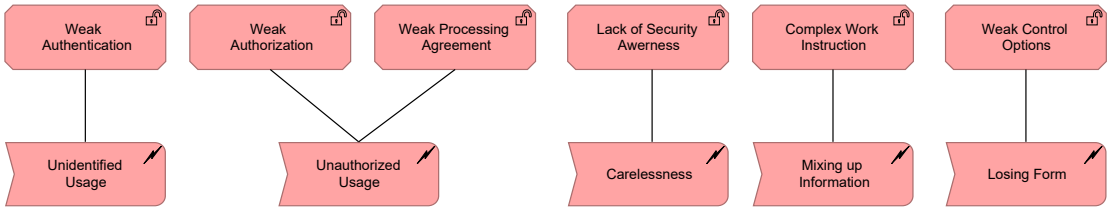

Fig. 7.17: Vulnerabilities and Threats

Unidentified usage

Weak authorization can lead to unidentified usage of services. This is a threat since you can't be sure the usage of the service is legitimate. Especially services serving access to personal information are vulnerable for this threat.

Unauthorized usage

Even when identified weak authorization can become a threat. The unauthorized usage of a service can happen with this vulnerability. A threat agent could have access to assets he shouldn't have access to and do harm.

Carelessness

The lack of security awareness is a vulnerability which can lead to carelessness. This carelessness is a threat where for example an ignorant employee treats personal information like any other type of information while it should be treated confidential.

Mixing up information

Mixing up information is a threat where personal information is swapped or linked to wrong assets. This can for example happen when work instructions are to complex and are therefore wrongly executed.

Losing forms

The weak control options of printed forms can lead to losing these forms which means there is no longer control over the information on these forms. Some of the forms contain personal information and the forms are attached to equipment while being transported which makes this even a bigger threat.

Fig. 7.18: Risks

7.2.4 Risks

For organizations processing personal information there is no direct risk for any loss event. A loss of personal information primarily damages the involved individual. The motivation for organizations collecting and processing personal information to do this carefully is a result of privacy regulations. Not adhere to privacy regulation will eventually result in a financial sanction. This financial loss is a major risk for organizations that don't cope with the vulnerabilities in their organization in an appropriate way.

Another risk for organizations is the risk of reputational damage. Losing personal information often generates a lot of attention from the public since the information lost is directly related to the public. Besides, organizations are often obligated to inform the individuals whose information it entails when a leakage has occurred. This reputational damage can also be seen as a risk, especially since it can create the image of an unreliable business partner. Municipalities for example will and have to choose reliable business partners.

Every threat defined in the previous step can lead to a loss event. The risk is defined by the frequency of loss events and the impact of a loss event. The more impact a loss event has and the higher the frequency of a loss event, the higher the risk. All loss events resulting in the loss of personal information have impact on the risks as described above.

7.2.5 Security policies and principles

When the risks are identified the first phase of the risk assessment is completed. The second phase of the risk assessment focuses on the deployment of security measures to mitigate the identified risks. The first step of this process is to define and map the security policies and principles.

The security policies and principles capture the 'risk appetite' of an organization, what level of risk is an organization willing to accept? The principles are a high level view of an organization's security apatite. Such a high level principle can for example being compliant with rules and regulations. Applying this principle on the current scope results in the following principle:

> *Comply with privacy rules and regulations*

Security principles are usually high level expressions of an organization's risk appetite. But stating that you as an organization will be compliant with privacy rules and regulations is still a bit vague. Because what does it mean, when do you comply with these regulations? It can maybe be more helpful to further explain what it means to be compliant by also trying to map the elements of the privacy rules and regulations.

In order to be compliant with the privacy rules and regulations an organization has to adopt the restrictions as stated in the privacy legislation. The policies can be a representation of the restrictions regarding the collecting and processing of personal information as stated in privacy regulations. For the Netherlands the collecting and processing of personal information is regulated by the WBP. Many of the restrictions of the WBP can be mapped as organizational security policies to which the organization has to fulfill in order to be compliant.

The policies are an interpretation or practical implication of the regulations as stated in the WBP and GDPR. The preconditions for the legitimate processing of personal information are covered in chapter 2 of the WBP, articles 8 up to and including 14.

WBP article 8 states that the processing of personal information is only allowed when one condition is met in a set of conditions. One of this conditions is that processing is allowed when the subject has given permission. Another is when the processing is on a legal basis. These two preconditions are applicable to this scope, since the delivery of medical equipment is either a commercial sale with a user agreement or a delivery based on one of the social health care acts. This article will therefore be summarized in the following policy:

Only process personal data when the subject gave permission or when there is a legal basis

Article 9 further limits the collecting an processing of personal information by stating that only the information needed to execute the predefined goal is allowed to collect and process. No unrelated information may be collected or processed. This is important because this means that once you have permission to process personal information this doesn't mean you can process all personal information. The following policy captures this restriction:

Only process personal information required to execute a predefined goal

As an addition to the previous articles article 10 states that the processing of personal information is only allowed for the time it is required to execute the original goal. This means that any processing of personal information while the goal is fulfilled is prohibited. The following policy captures this behavior:

Only store personal information for the time it is required

According to article 11 the processing of personal information is allowed for the goal it is collected for. When someone has given permission to process your personal information for the execution of a sales agreement the information may only be used in processes directly related to this goal. The following policy will cover this restriction:

Only process personal information for the goal it was collected for

Article 12, 13 and 14 are about the processing of personal information by third party partners. These can be any kind of partners, for example: suppliers, clients, partner who execute parts of the process, or parties involved in the implementation and support of information technology. When third parties are involved the one responsible for the collecting and processing of personal information is also responsible for the responsible processing of personal information by these parties. The third parties have the same responsibilities as the party who provides them with personal information. Only information needed to execute the processes they are contracted for should be shared between the partners. The special attention for third parties involved is captured in the following policy:

Processing of personal information by third parties is under strict measures

The general articles of the WBP are all covered by a policy but some additional articles of the WBP can and should also be covered by a policy. First of all there is a category of personal information explicitly mentioned in the WBP, the sensitive personal information. This category includes personal information related to different subjects with, among others, information about someone's health. The fact that someone uses medical equipment can already be classified as sensitive personal information, let alone the information needed to correctly assess clients' needs. Articles 16 and 21 of the WBP are covered by the following policy:

Only collect and process sensitive personal information when explicitly allowed

The WBP also already mentions personal identification numbers. Although further restrictions and clarification of the usage of the national personal identification number is covered by another act, the BSN, the WBP already gives some direction about how to handle these numbers. The usage of a number to identify a person as prescribed by law is only legal when explicitly allowed. This article 24 of the WBP is covered by the following policy:

Only store personal identification numbers when explicitly allowed

An advantage of this approach is that every policy can directly be linked to a paragraph or statement in the privacy act. This mapping is visualized in (Tab. 7.1). The identified principle and policies can also be modeled in the ArchiMate language. This model is presented in (Fig. 7.19)

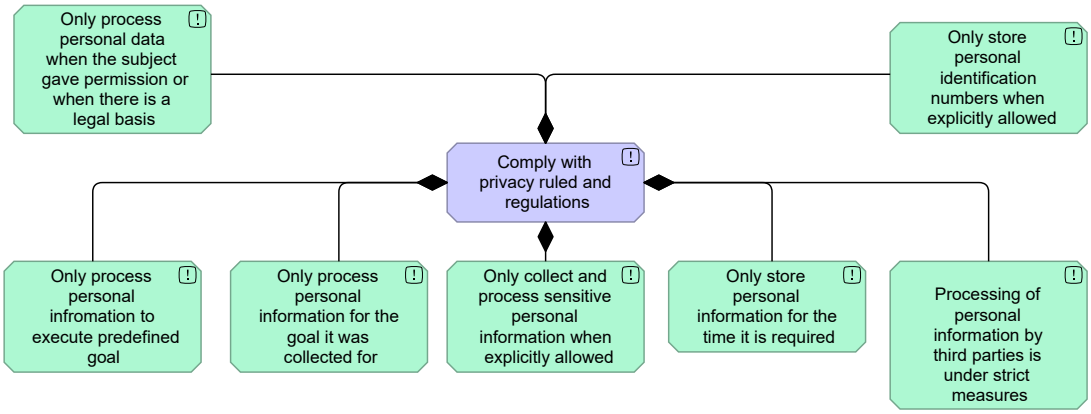

Fig. 7.19: Principle and Policies

Policy	WBP article no.
Only process personal data when the subject gave permission or when there is a legal basis	8
Only process personal information required to execute a predefined goal	9
Only store personal information for the time it is required	10
Only process personal information for the goal it was collected for	11
Processing of personal information by third parties is under strict measures	12, 13 & 14
Only collect and process sensitive personal information when explicitly allowed	16 & 21
Only store personal identification numbers when explicitly allowed	24

Tab. 7.1: Policies mapped to WBP articles

For now, only policies which are directly linked to articles of the WBP are taken into account. But other privacy norms can easily be mapped the same way. Like the agreed upon partner agreements or restrictions which are a result of the processing agreement. But also company wide principles and policies regarding the processing of personal information that are possible stricter or more specific than national rules and regulations. All can be presented as principles and related policies and further specify the risk apatite of the organization.

7.2.6 Control Objectives

Control objectives are high level security requirements. The control objectives are based on the outcome of the risk assessment and predefined security policies and principles. They should mitigate the identified risks. These control objectives are the starting point for the definition of the requirements for the control measures.

It can be helpful to use a predefined set of control objectives like the ISO 27001 control objectives or the control objectives as defined in COBIT 5. The ISO 27001 control objectives are designed to mitigate the risk and increase information security. Another advantage is that when the control objectives of these standards are met an organization is one step closer to ISO 27001 compliance.

We have to select a few control objectives as listed by ISO 27001. The total list contains 35 control objectives divided over 14 groups. Not all control objectives are directly related to the scope of this project and will therefore not mitigate any risks as assessed during this process. The ISO 27001 control objectives are designed to increase overall security, while this risk assessment focuses on privacy issues. When possible and necessary the control objectives will be adjusted and defined so they cover these specific issues. Keeping the above conditions in mind the following selection of control objectives can be made.

Emphasize security during employment (ISO 27001 - 7.2)
This control objective should ensure that employees act according to the applicable security principles during their employment. This objective is as important as having the security principles itself. Actively emphasizing the importance of security during employment has a positive effect on the actual security.

Respect business requirements (ISO 27001 - 9.1)
The access to all assets where personal information is processed should be controlled. Uncontrolled access should be impossible since you can't check whether the access is legitimate and according to the business requirements.

Manage all user access rights (ISO 27001 - 9.2)
Every user should only be authorized to access assets he needs to use to execute their tasks. For every user or user group the activities he or she should perform are known and the access to assets should be limited to this list.

Protect user authentication (ISO 27001 - 9.3)
The credentials used by users to authenticate themselves are secret and only known by the user. The user himself is responsible to keep the credentials secret. This objective makes it possible to make users accountable for actions performed by him.

Control access to systems (ISO 27001 - 9.4)
Only authorized user should have access to services and systems processing personal information they need to execute their tasks. The unauthorized access to systems and services shouldn't be possible.

Use logs to record security events (ISO 27001 - 12.4)
To make individuals accountable for actions they perform logs should be recorded. When

accessing personal information or adjusting it a log record should be stored. These can be used to audit the performed actions.

Establish security agreements with suppliers (ISO 27001 - 15.1)
To protect personal information and related assets which need to be shared with suppliers or other third parties there has to be an agreement about the level of security.

7.2.7 Requirements for control measures

The control objectives and the security principles and policies together form the basis for the control measures. The requirements for the control measures are examined in this section. The control measures are proposed solutions and are used to realize the control objectives. All control objectives and policies should be covered by control measures to make sure the objective are achieved. The control measures are also linked to vulnerabilities. The control measures reduce the level of vulnerability of the vulnerabilities depending on the control strength.

Strong authentication procedures
A strong authentication procedure should make it impossible for others than the one who has the secret credentials to identify himself. This measure fulfills multiple requirements. First of all it makes it possible to make individuals accountable for actions they perform. This is a precondition for audit trail logging, which is a separate control measure. Strong authentication procedures are also a precondition for a strong authorization process. Only authenticated users can be authorized to have access to assets.

Update and improve access control policies
The access control policies should represent the business requirements. This means there has to be a clear distinction between business roles and a their permissions. The permissions have to meet the restrictions as imposed by the privacy law and regulations.

Review user access control list
This control measure should ensure that services that provide any kind of personal information are only accessible by employees who need the information to perform assigned tasks. This requires an access control list defining who needs access to which assets. This access control list should be based on the principle of least privilege meaning that access is only given when needed to perform intended functions. The definition of the access control list should be continually improved to match the business requirement and to keep up with employment changes. The level of detail can be matter of discussion since the authentication can be defined on groups of assets, assets or instances of assets.

Develop secure external communication policy
Information sharing with third parties has to be strictly controlled and secure. This control measure should focus on all processes where there is some kind of communication with third parties. This means that both the communication with the customers as well as the communication with the transportation company should be covered by this measure.

The communication is secure when only that information is shared that is needed by the external party. Secondly there should be appropriate tools available for secure communication.

Eliminate paper usage
The control over printed information is weak and one way to reduce this vulnerabilities is to eliminate paper usage in all processes. There are multiple solutions available that have better control options available. To be able to manage all access rights to personal information

Standardize contracts
To reduce the complexity of some processes it is an option to standardize contracts with applicants. This control measure has a lot of impact and the design of this control measure will probably be difficult. But this is a measure reducing the vulnerability regarding complex processes.

Continues privacy awareness program
To improve the security awareness of employees and to emphasize the importance of privacy during the employment the implantation of a continues privacy awareness program should be considered. The employees are an important key to achieve overall protection of personal information. This control measure aims at the general human intention to comply with regulations. It should reduce the level of vulnerability regarding the lack of security awareness.

Time limit personal information storage
Stored personal information has a expiration date by law meaning that when personal information is no longer needed and the original goal for what it was collected for is fulfilled the information should be destroyed. This is an activity that isn't executed automatically and a process should be in place to achieve this.

7.2.8 Design of control measures

With the actual design of the control measures we try to implement these measures into the organization. The design of control measures also depends on the current enterprise architecture. For the design of the control measures many design choices have to be made. Control measures can be implemented in different ways.

Take for example the control measure: eliminate paper usage. This control measure has impact on every process where paper is used. And for every process where paper is used there are different solutions imaginable to replace the paper forms. First of all you can maybe fix it by redesigning the business process. This means that for example responsibilities and tasks are relocated so the paper forms aren't necessary any longer. Another solution may focus on the implementation of an application or the redesign of an existing application to replace the function of the paper form. Besides, there are many (non-)functional requirements that have to be met that are currently unknown before any of the solutions can be designed and implemented.

Since there are so many different ways to implement the control measures a full list of all projects with a designed solution of the proposed control measures isn't feasible. But we can give an example of how a designed control measure would look like and could impact the monitored baseline architecture.

7.3 Summary

The executed analysis first of all gives us a detailed view on the basic request handling process at Welzorg. Secondly and evenly important it demonstrates how the designed artifact, the privacy risks and personal information management methodology, can and should be used to analyze business processes and related it components. In the next chapter we will look at the implications of the executed analysis. First of all we will look at the implications for Welzorg, secondly we will look at the performance of the designed methodology in general.

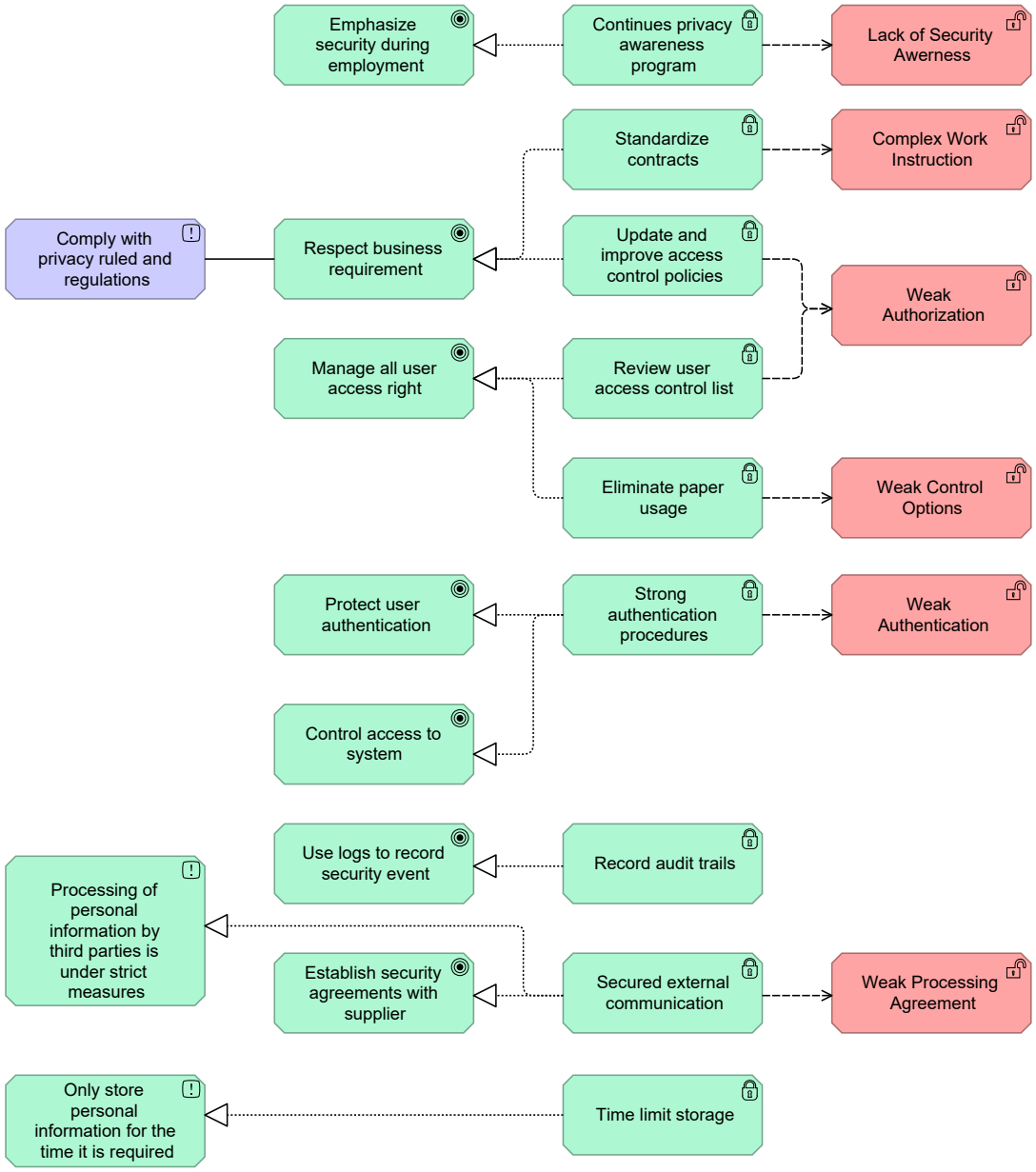

Fig. 7.20: Control Measures

8 Welzorg practical implications

8.1 New projects

As indicated with the execution of the methodology at Welzorg there are some control measures that should be implemented in order to reduce the impact of vulnerabilities an therefore mitigating the risk. In this section the projects will be discussed that should implement these control measures. Only three projects are highlighted. These projects are chosen based on informal interviews with Welzorg employees.

8.1.1 Centralized authentication and authorization

Two vulnerabilities that are present in almost every monitored process are the weak authentication and weak authorization. But on top of the monitored processes these vulnerabilities seem to be present in many more processes. The cause being the missing of a centralized authentication and authorization systems.

Currently there are some processes in place to make sure only authenticated and authorized users get access to services they need to perform work. Every application has its own authentication system. This means that a user that needs access to services provided by a particular application gets a user name with password. Whether an employee gets an account for an application is based on the so called Function Application Authorization Matrix (FAAM). Based on the function of an employee it can be decided whether the employee needs access to an application. The employee will get an account with rights as described in the matrix.

What makes the current authentication and authorization process vulnerable is the usage of different accounts for different applications. An employee that has to have access to several applications will therefore have to remember multiple authentication credentials.

Another factor that makes the authorization process vulnerable is the way the rights are provided. There are many steps that are executed manually. Some of these steps are done manually as an extra check to increase security.

A centralized authentication and authorization system will reduce some of the identified weaknesses. With a centralized systems all application share an authentication service. Every

employee will only have one set of credentials to authenticate himself. When the authentication is centralized the management of the policies also becomes easier. New policies like the usage of two factor authorization or longer passwords have only to be implemented once.

By centralizing the authorization the providing of access rights is also less sensitive for mistakes. It is easier to keep the user access rights up to date when managed centralized. In the current situation the authorization levels have to be updated for every application when an employee's rights change.

Revise permissions

Although a centralized authentication and authorization service has a high priority it doesn't fix all weaknesses related to authorization vulnerabilities. A next step in reducing the authorization related vulnerabilities is updating authorizations for each application service. Currently, for some applications only permissions to write are defined. Take for example applications that are part of the Oracle ERP suite. The users with an account are only limited to perform certain functions within the application, but can read anything within the application. From a privacy viewpoint the permissions to read information are maybe even more interesting. This means the permissions within applications have to be revised to match the business processes. A special interest should go to read permissions regarding personal information.

8.1.2 Continues privacy awareness program

What became clear during the execution of the methodology at Welzorg is that there is little privacy awareness among employees. This while employees are often seen as the weakest link in a secured environment. This lack of awareness goes for the whole organization on every level. While the nature of people is to be compliant with regulations, the intention to comply is high. So we can conclude the employees are just not aware of the risks that comes with the processing of personal information.

A privacy awareness program has to make the employees aware of the kind of information they process, which is personal information, and the responsibilities that come with it. This awareness program should make clear that when dealing with personal information extra caution is needed. When processing personal information this information should be handled with care and when distribution this information an employee should for example double check the recipient.

A possible down site of a privacy awareness program is that employees become over protective which has impact on the productivity. Another possible down site as identified during interviews is that employees become protective towards auditors regarding their way of working. It is important that employees keep being honest about all actions they perform, especially those

related to the processing of personal information. Otherwise the vulnerabilities that are possibly related to these business processes stay unknown. These possible down sites must be taken into account when implementing the privacy awareness program.

8.2 Impact on existing projects

8.2.1 Master Data Management

Master Data Management (MDM) has become quite popular in many organizations (Howard, 2013). At Welzorg and the parent company, Louwman Group, with his subsidiaries there also has been some discussion about the implementation of a MDM system. The goal of the implementation of MDM is achieving consistency. A MDM system ensures everyone in the organization has access to the same information. This maybe seems evident but organizations often use many different applications which all support different business processes and therefore process different sets of information. Many applications use a dedicated database storing this information resulting in overlap in the information stored by application within an organization.

An integrated MDM approach can eliminate these shortcomings. Using an MDM tool has multiple advantages. Having a single source of information reduces mistakes made by having duplicate or de-normalized information available. But the implementations of a MDM also has some risks. One single source of information means that all information related to an object is linked to this object. Linking information and thereby enriching the value of information increases the risks regrading privacy. Personal information is better protected when isolated.

But keeping the current situation where information is distributed over multiple applications because otherwise the information becomes too valuable is a form of security by obscurity. The information is already available in the organization. Centralizing the information management has more advantages than disadvantages.

Data portability and right to be forgotten

Some of the advantages are actually related to the new privacy regulations. When the GDPR becomes active data subjects get more rights regarding their personal information. Compared with the current situation individuals can have more control over their personal information. Individuals already have the right to request organizations to get all personal information that is processed by that organization. But what is new is that the right to data portability. This means that the requested information should also be available in a commonly accepted machine readable format.

A second right of the subject is the right to be forgotten. This means that an individual can, in some cases, request an organization that has previously processed his personal information to remove this information.

For organizations processing personal information this means they have to be prepared for these requests. When MDM is implemented fulfilling these request don't have to be hard. Removing or correcting personal information from applications when an MDM is used should be easy since there is only one source of this information. Currently, such request would be much harder since the information is distributed over multiple applications.

Dell Boomi

With the implementation of a data integration layer at Welzorg there is already a move toward an MDM approach. When the exchange of all data between applications goes through a single hub a logical next step is to apply MDM on this hub. Currently Welzorg uses Dell Boomi as a hub for the integration of data between applications. New developed applications that need information that is available somewhere else in the organization have to build an interface with Dell Boomi to get this information.

8.2.2 Working paperless

Sustainability and availability of information are for many organizations reasons to reduce or eliminate the usage of paper. Welzorg has also indicated that it wants to reduce and eventually eliminate the usage of paper forms. Based on the privacy risk analysis another important driver can be identified to start such a project. The access control capabilities of paper are low. Applying authentication and authorization before accessing information printed on paper forms is hard. When a printed form lies on a desk a solid identification of everyone who tries to access the information on this form is impossible. Besides, such printed forms can easily be lost. This is especially a threat during the processes as monitored where physical forms are used: during transportation. Especially since the transportation is partly done by a third-party and in an uncontrolled environment.

So, there are many reasons to get rid of the use of paper forms. Especially in the processes where they are currently used. Many technical solutions are already available that makes a migration towards a paperless working space easier. The carriers for example already have a PDA used during the delivery of the equipment. But the solution doesn't have to be technical. For the sorting of the goods at the VNS's you can ask yourself what information is needed. Maybe it is enough to label the equipment to make clear which carrier should take which equipment. The label only has to have information about which carrier should take the equipment. This won't contribute to the goal of working paperless (the labels are still printed), but at least there is no longer personal information printed.

8.2.3 Applications under development

The executed analysis has also impact on some applications that are currently under development. Multiple new applications are under development. One of which is an applications that should replace multiple applications used by the customer service desk. Another application under development is an application for order pickers in the warehouse.

The development of these application was parallel to the conducted research as covered by this paper. Some of the insights as collected during this research have already been implemented. With the development of these applications the privacy aspects are taken into account and the protection of personal information is a topic now. This in contrast to when the current applications were developed.

But since the applications are still under development they don't cover all processes and exceptions. This why the current applications are still used in an addition to the newly developed ones. The motivations to develop the new applications were primarily to be more productive by developing an application that better fits the business processes. But from a privacy perspective the migration towards the new applications is also recommended. The permissions regarding the personal information processed by these applications are better manageable, especially the one used by the customer service desk.

For applications or services that are developed in the future the privacy principles and policies as defined in step 5 of the executed methodology can be helpful. They capture the essence of the privacy rules and regulations in as practical applicable policies. Every applications or service that somehow processes personal information should have these policies as non-functional requirements.

8.3 Limitations

8.3.1 Enterprise architecture

The execution of the methodology is strongly based on enterprise architecture principles. The distinction made between layers and the focus on the how business processes are supported by applications are typical for an enterprise architecture look at an organization.

At Welzorg there is no enterprise architect appointed neither is there someone with a similar role. This can be identified as a shortcoming. An enterprise architect ensures cohesion within an organization between requirements. With a holistic view on the organization the enterprise architect should make sure that the business and the IT are aligned. Enterprise architects make sure that individual projects fit in the organizations, both from a business perspective as

well as from a technical perspective. Tools that support an enterprise architect are different architecture views. An enterprise architect knows exactly how the current architecture looks like, how the target architecture looks like and which implementations and migrations are needed to get there.

As illustrated with the case study an enterprise architecture approach is also useful during a risk assessment. But currently the added value of this approach is minimal due to the lack of enterprise architecture management at Welzorg. The models that illustrate the baseline enterprise architecture should match the current situations at an organization. Therefore, they need to be updated constantly. Together with an enterprise architect the execution of the privacy risk assessment becomes much easier. This is why, from a privacy perspective, it is recommended to assign one.

8.3.2 Identification of vulnerabilities

During the execution of the privacy risk assessment one particular activity was hard to execute. The identification and formulation of vulnerabilities of assets. First of all the problems with the identification activity. The vulnerabilities covered by the privacy risk assessment are now identified based on feedback and talks with employees of Welzorg or based on common, well known general vulnerabilities. This can be classified as a rather weak approach and not very systematically. Although many vulnerabilities could be identified this way with a more systematic approach can increase trust in the coverage ratio of the identified vulnerabilities.

The first proposal to strength the identification activity is to keep track of issues an breaches that occur in the future. Currently Welzorg doesn't keep track of issues that occur. It was therefore hard to make sure the all vulnerabilities that in the past had led to actual losses were covered. The implementation of an central issue tracking to keep track of all privacy related breaches can prevent this in the future. Such a tracking system makes sure the vulnerabilities don't get out of sight and eventually appropriate counter measures are taken to address the vulnerabilities.

Another measure that could be taken to strengthen this activity is to execute a penetration test. A penetration test Bishop (2007) is a tool that can be used to analyze aspects of a system. The goal of a penetration test is to identify whether the system has vulnerabilities that can be exploited to do harm. The penetration test is a simulated attack on the system to test whether appropriate control measures are taken to protect the system. In the context of the privacy risk assessment at Welzorg such a test will purely focus on personal information and getting control over this information. The system under attack will be the system as described by the enterprise architecture. Typically such a penetration test is executed by an external actor who uses techniques that any threat agent could use to initiate an attack. Vulnerabilities identified by the test can be mapped on the enterprise architecture.

8.3.3 Limited scope

The current privacy risk assessment focuses only on personal information of clients as is according to the chosen scope. But it is important to note that the privacy rules and regulation, WBP and GDPR, make no distinction who's personal information it concerns. The collecting and processing of all personal information of all individuals is protected by these laws. An important set of personal information out of scope of the executed assessment is that of the employee's. The business processes dealing with this personal information stand alone, they have no direct relation with the operational processes such as the basic request handling.

An important reason the employer's personal information is out of scope for this project is that Welzorg or organizations like Welzorg are not unique in the processing of this information. Every organization processes personal information of its employees. It can be argued that the approach introduced in this paper can be used to assess the risks associated with the processing of employee's personal information. But this will not be further highlighted. It is worth noting that the amount of personal information of clients processed is much higher since Welzorg has more clients than it has employees and some health related information is processed for the clients.

The scope was also limited to the business and applications layer. The main argument to limit the scope to these layers was that privacy specific related vulnerabilities would only occur in these layers since vulnerabilities related to technology assets would expose general security risks. Although these general security risks also should be mitigated and some will also be related to risks regarding privacy for the assessing and controlling of these risks are general security management methodologies available.

8.3.4 Qualitative analysis

Also out of scope was the qualitative analysis. A qualitative analysis can help to classify the risks by making it qualitatively measurable. By determining the impact of a possible loss and the frequency of such an event the risks can be ranked. Based on this ranking the importance of the control measures can be determined. With this approach you can also make the risk apatite measurable. What level do you as an organization accept?

The impact of a loss event together with the frequency of such an event determine the risk level. A loss event is an actual negative impact caused by a threat. The threat on his turn uses a vulnerability of an asset. The level of vulnerability is determined by strength of a control measure and the capability of a threat. The loss event frequency is determined based on this level of vulnerability and the threat event frequency. The magnitude of loss event and the frequency of the loss event together determine level of risk (Jonkers and Quartel, 2016).

Such a detailed explanation of the risks and which factors are accountable for the level of risk can be very useful. When it becomes clear which vulnerability is accountable for which level of risk you can make a motivated choose about which control measures should be implemented first. However, to do so you need a lot data to do the calculations with. Collecting all the data to identify the values of the variables that are needed to calculate the level of risk costs time and is a project in itself.

8.4 Achieved Goals

8.4.1 Customers

Questions regarding the processing of personal information by contracted organizations like municipalities were a main reason for Welzorg to perform a privacy assessment. These contracted organization provide a lot of the personal information processed by Welzorg and they want to be reassured that Welzorg has taken appropriate measures to protect the privacy. Currently, Welzorg isn't fully sure how to deal with the different requirements made by the municipalities. This resulted in a situation where Welzorg had different agreements with various municipalities about for example how to safely communicate about clients and share personal information.

The demands made by the municipalities were leading while these demands vary between municipalities and not all proposed measures fitted the objectives. A more clear statement towards how Welzorg deals with personal information has two main advantages. First of all, with an unambiguously policy regarding the collecting and processing of personal information Welzorg continues to be a trusted partner. It shows the organization takes privacy seriously and knows how to deal with the responsibilities that comes with being a processor.

Secondly, now it's clear what being compliant with the privacy regulations means the solutions for operational challenges can also be properly selected. A more unambiguously set of solutions is easier to implement and maintain. But the main advantages is the clear communication towards municipalities about solutions supported by Welzorg that comply with the privacy regulations. This should prevent that every contracted organizations comes with his own solutions.

8.4.2 Compliance with GDPR

The most important motivation for this research was the shift towards new privacy regulations. When the GDPR becomes active in 2018 organizations like Welzorg that collect and process

personal information of many individuals have to deal with this information even more carefully.

Privacy Impact Assessment

One of the most important changes as a result of the implementation of the GDPR is that processors of personal information are obligated to demonstrate compliance with privacy regulations. For some organizations this even means that they have to execute a privacy impact assessment (PIA). A PIA is an instrument used to systematically identify risks associated with the collecting and processing of personal information. The execution of a PIA is mandatory for organizations that process personal information in a special category, like the health related information. This means an organization like Welzorg should execute a PIA since they process health related personal information.

The privacy impact assessment is mostly about awareness. An example of how to execute such an assessment is given by NOREA (0011–2015). An important element of this assessment is a questionnaire. By filling in this questionnaire an organization can determine the impact of the processing of personal information. Many of the information needed to answer these questions can be derived from the analysis as executed at Welzorg. By analyzing all core business processes the same way as the basic request handling many information is collected to answer the PIA questionnaire and thereby to fulfill the assessment.

8.4.3 Health records

Personal information related to someone's health is classified as special personal information. This is a rather broad definition. Information can be classified as related to someone's medical condition pretty fast. At Welzorg, the client's information used to do the assessment as well as the order for the equipment can be classified as medical personal information. The information needed to do execute the assessment with is in many cases information about someone's medical condition. The same goes for the order information: the fact that someone needs medical equipment is personal medical information.

Personal information classified as special personal information requires special attention. This means that business processes that access this information should be closely screened. The assessment information and the order information contain personal information that isn't directly related to an individual. That means that as long as they are processed separate from the client information they don't expose any personal information. It is therefore important to separate the client information from other sets of information. This reduces the impact of vulnerabilities related to assets processing these sets of information.

With the executed privacy assessment these assets can easily be identified.

8.4.4 Usage of BSN

The Dutch national identification number (BSN) has been discussed earlier. The BSN is a unique number related to a Dutch citizen with a special status. It is primarily used by governmental institutions to uniquely identify citizens. Some private organizations are also allowed to use the BSN, but only in some regulated cases.

By limiting the scope to WMO request the BSN has been out of scope. For the execution of the WMO there is no exception in the Dutch law to use the BSN. For the execution of the ZVW or the WLZ for example there is an exception. This means that it is allowed to uniquely identify clients that require equipment covered by these health acts based on their BSN. So using or storing the BSN of clients that require WMO covered equipment isn't allowed. But unfortunately this doesn't mean that the BSN hasn't be used in the communication with municipalities to uniquely identify clients.

That it is allowed to use the BSN for identification during the execution of some of the health care acts can be the origin of this misusing. It doesn't help that a communication standard designed to standardize the communication between municipalities and health care providers requires the clients to be identified by their BSN. In all standardized messages of the iWMO the BSN is an obligated field. The reason it is designed this way is probably because it is based on other standards used in the health industry. But these standards are used to communicate about health care covered by other health care acts.

Another complicating factor is that different municipalities use different communication channels. With the different types of contracts that municipalities can have with Welzorg come also different agreements on how the communication is organized. The different types of contracts were also identified as the source of a vulnerability: wrong execution of work instructions. Some communication is done through email, some through special external portals and some through a portal maintained by Welzorg.

Although some will argue that using the BSN during the execution of the WMO should be allowed for the same reasons it is allowed during the execution of the ZVW and WLZ it currently isn't. This means that municipalities that share the BSN during the execution of the WMO are violating the law. Some municipalities have been reproved by the privacy authority for the usage of the BSN (Asser Courant, 2016).

Replacing the BSN by another unique identification number would be a solution. But this solution may seem easier than it is. Since there are so many different municipalities involved that all have to adjust their way of working the migration will probably take some time. For Welzorg it is important to at least limit the usage of this BSN for the WMO request as much as possible. Secondly, Welzorg has to be prepared for an alternative way to identify clients.

8.5 Summary

This chapter sums up the control measures that help Welzorg to become compliant with privacy rules and regulations. First of all some new project should be started. A centralized authentication and authorization system will reduce mistakes and unauthorized access. By managing the permissions to applications in a central place the unintended access to application with sensitive information will reduce. Secondly, a continues privacy awareness program helps to make the employees aware of the sensitivity of the personal information they handle. As a result the employees will handle personal information with more care.

Every database and every document containing personal information should be under strict control. It may therefore be useful to implement Master Data Management. With one single source of truth in a central place the protection and control over personal information will increase.

A final control measure that should be worked out is the paperless office. At least there should no longer be any printed forms with personal information on it. It is hard to control who has access to these papers. Therefore all personal information should be shared and stored digitally when possible.

9 Discussion Methodology

In this chapter I will discuss the proposed methodology. The experiences gained with the execution of the methodology at Welzorg will be evaluated. When possible and necessary improvements to the methodology will be proposed. Five topics will be discussed in this section. First of all the chosen views and how they are visualized with ArchiMate. Secondly, the process of identifying the vulnerabilities and threats. Next topic of discussion will be the privacy rules and regulations and how they are incorporated in the assessment. Another point of discussion will be the decision to build the privacy risk assessment on the existing methodology of Jonkers (2014). Finally, the individual steps of the methodology will be discussed. Especially whether each step is useful to execute or not.

Feedback regarding the applied methodology was collected during several sessions. First of all feedback was collected during interviews with the IT manager at Welzorg. Secondly, the methodology, case study and practical implications were presented at Welzorg to a group of stakeholders. The group of stakeholders existed of the IT manager, the compliance officer, a privacy expert, the GRDP project manager and the marketing director. After the presentation feedback was collected during a round table discussion. Feedback collected with both methods were used as input to for this chapter.

9.1 Chosen views and modeling elements

An important element of the methodology are the defined views. The ArchiMate views should give a good representation of the addressed concerns. They should give meaningful insight in those parts of the organization that matter for the executed analysis.

Especially two views give a lot of meaningful insight. The first view that does so is the one that supports the monitoring step. All elements that are important for the execution of the business process in the center are presented in this view. In one view it is clear with actors, application services and business objects are involved. By going step by step through all business processes no elements are missed. All views together give a complete view of the investigated high-level business process.

Another feature of this view is that business actors can empathize with the illustrated process. The business actors are important stakeholders when it comes to the vulnerabilities. By

dividing the high-level business process into small business processes they can be linked to single business actors.

The second view that gives a lot of meaningful insight is the view where the vulnerabilities, control objectives and control measures come together. This view contains a lot of elements but it clearly illustrates how the vulnerabilities are mitigated by control measures which on their turn are an implementation of the control objectives. This view actually illustrates the core of the analysis: the alignment of the control measures with the identified vulnerabilities.

These two views together give the most insight in the current state of the enterprise regarding privacy related risks.

Besides the chosen views it is important to evaluate whether the chosen modeling language, ArchiMate, supported all elements that had to be modeled. The current version of the modeling language has elements included specifically for the modeling of risk related elements such as vulnerabilities, threats and security principles. The available elements were sufficient to model all privacy risk related elements.

There should be a clear connection between vulnerabilities and control measures. In the end you try to control the vulnerabilities with control measures to reduce the risks they expose. I believe this relation is an important element of the modeling language and should therefore be highlighted. A relationship that has been subject of discussion is the relationship between a vulnerability and an application service. Is it possible for an application service to have vulnerabilities? Although in the end the vulnerability may be an issue deeper in the architecture, in the technology layer or a more detailed application asset, the vulnerability arises in the application service. Besides, an application component can have several application services which do not necessarily expose the same vulnerabilities. Especially in the case of privacy related vulnerabilities where some services do serve personal information and others don't.

9.2 Vulnerabilities and threats

One of the key steps is the identification of the vulnerabilities and associated threats. These steps are also the most difficult ones to execute for several reasons. I will discuss weather the chosen methodologies and frameworks were sufficient and easy to apply in a case study.

Identification

The actual identification of vulnerabilities is done based on interviews and the analysis of the monitored assets. Together with a list of common occurring vulnerabilities this step can be completed. But it feels a bit like defining vulnerabilities from thin air, which would

mean that not all vulnerabilities are covered. Besides, there can be many different kind of vulnerabilities, which makes the structured search for these vulnerabilities hard. The analysis doesn't result in a conclusive list with vulnerabilities. Instead, the analysis gives direction and structure to the search for vulnerabilities. But in the end the completeness of the list with identified vulnerabilities depends on how well the business processes are understood and general knowledge of possible vulnerabilities.

Another problem is that some vulnerabilities are only vulnerabilities because it exposes a situation that is not compliant with rules and regulations. Take for example the regulated limited storage period of some personal information. For many types of information this isn't a problem, but for personal information it is. Therefore such a vulnerability will not be mentioned in lists with common vulnerabilities. For these assets it is not only important to know where in the organization they are used, which is investigated by monitoring the parts of the organization, but also the restrictions of these assets.

Definition

Besides the above mentioned difficulties there were some other challenges with the identification of the vulnerabilities and threats. Not only was hard to identify the vulnerabilities but it was also hard to define the vulnerabilities and to link them to the correct asset.

First of all the definition issue. This may seem a bit niggling but by choosing the wrong definition the vulnerability isn't properly addressed. When wrongly defined the vulnerability may not seem to be vulnerability of the asset it is associated with. In other words, the defined vulnerability must be an actual vulnerability of the related asset. By wrongly defining the vulnerability it may seem that the vulnerability isn't linked correctly and therefore exposes not the threat it really does. A model is always a simplified representation of the real situation. But the important aspect should be modeled as close to the real situation as possible.

Another challenge related to the definition issue was the ongoing consideration between what a vulnerability and what a threat was. In early sketches of the views related to the risk assessment part of the methodology vulnerabilities and threats were used mixed. While in theory there is a clear distinction between those two. A vulnerability is 'just' a weakness of an asset, the threat is the misuse of the vulnerability. A vulnerability can be an inadequate protection of an asset and a related threat can be the misuse of this inadequate protection. Or take for example the unauthorized use of an application service, a threat, which can be related to weak authorization protocols, the vulnerability.

Understanding the distinction between vulnerabilities and threat is maybe the core of the risk analysis. By correctly defining the vulnerabilities the root cause of the risk can be eliminated. Otherwise you are fighting the problem and not the source of the problem.

The final challenge was the linking of the vulnerabilities to the correct asset. A vulnerability is a weakness of an asset, but of which asset? This was often a point of discussion during the execution of the analysis. The first reason for this being a problem may be the limited scope of the analysis. Not all assets available in the organization were modeled in the chosen views. We choose to link the vulnerability to the asset that exposes the vulnerability in the modeled views. The current level of detail of the chosen views as well as the broadness of the scopes force us to do so.

In the Welzorg case study was some discussion about the vulnerability 'inadequate privacy awareness' of the employees. This vulnerability is exposed by the employees but is it really a weakness of the employees? Or is it maybe a weakness of the internal training program which results in employees not adequately being aware of privacy? Since the internal training program was not modeled in the current views and by choosing the definition of the vulnerability carefully it can also be linked to the employees. In the end it is a vulnerability that we should not ignore an lose sight of.

9.3 Privacy rules and regulations

Rules and regulations are by definition always applicable in general. This makes that the rules and regulations are applicable in many situations. But the general description of the rules and regulations makes them sometimes hard to interpreted and to understand how they should be implemented in practice.

The above goes also for the privacy rules and regulations. The laws protecting the privacy of individuals are rather general. This means that the laws don't state how the privacy laws should be interpreted, implemented or applied. Initially it is unclear how these laws affect certain domains and what measures should be taken in order to comply. No clear control measures are given in order to comply to the rules and regulations.

As part of the methodology I have tried to bring the privacy rules and regulations closer to the business processes. By incorporating the privacy rules and regulations as policies and principles in the privacy risk assessment the gap between theory and practice is one step closer. As a result the impact of these rules and regulation on how the business processes and information technology are designed or should be designed becomes a bit clearer.

By modeling the rules and regulations as policies and principles in the enterprise architecture views they become available in as enterprise architecture elements for future reuse. When (re-)designing parts of the organization and going through the ADM-cycle these elements can easily be reduced. This makes sure future developed parts of the organization are compliant with these rules and regulations.

Is the simple representation of the rules and regulations as principles and policies enough? Unfortunately it isn't. Some aspects of the rules and regulations are lost in translation. But at least the control measures that are partly an implementation of these rules and regulations have a clear origin in the enterprise architecture.

9.4 The methodology

For the analysis of the privacy related vulnerabilities we have chosen to apply a methodology based on the approach as defined by Jonkers (2014). This approach was defined on a high level of abstraction and defined for the execution of a general risk assessment. In this paragraph I will evaluate the decision to use this methodology for the execution of a privacy risk assessment.

As mentioned in the literature study the method follows other common and general methodologies used for risk management. The phases of the different risk management methodologies are similar. Unique is the extensive description for the security deployment phase, which is split in several steps. This makes this methodology very useful in practice since risks are not only identified but also mitigated.

There were no public case studies available that applied the ERSM. This application of the methodology was therefore a challenge. Jonkers and Quartel (2016) described which steps had to be executed to complete the ERSM but not in detail how these should be executed. How to execute such a methodology differs from scope to scope and area it is applied to. So it is understandable that the methodology didn't specify the 'how'.

Besides the discussion about the usefulness of some of the executed steps which will be discussed in the next section the ERSM is suitable for the execution of a privacy risk analysis. Since the methodology follows a general risk The element that makes Jonkers (2014) methodology the most powerful is the mapping between the architecture elements and the steps in the risk assessment. The visualization of the risk elements and the relation between these elements and the current architecture makes it easy to communicate about the identified risks. The visualization also helps to explain and understand the necessity of the implementation of control measures.

9.5 Usefulness of executed steps

The ERSM is a methodology that quite literally maps the risk taxonomy. The distinction made between a risk, a loss event, a threat event, a threat agent and a vulnerability is the basis of the ERSM. For the understanding of the concept risk this distinction is important. But for risk analysis in practice this distinction is a bit overkill. The tiny differences between the concepts

a vulnerability, a threat event and a loss event is for example, especially the latter two. A threat event is the misuse of a vulnerability and the loss event the actual event when a threat agent abuses such a vulnerability. The result is a list of events: weak authorization can be misused which results in unauthorized usage. This threat can possibly lead to an actual event of unauthorized usage.

The goal of the execution of the methodology was to identify vulnerabilities and to select appropriate counter measures. All executed steps should contribute to this goal. Some steps can maybe be skipped for the practical approach. The detailed risk analysis can be more compact. It is maybe a bit excessive to analyze all possible threats and loss events. That weak authorization can lead to unauthorized usage may be evident.

So, for the understanding of the risk concepts it is good to make a separation between the different steps. But for a practical execution it is not necessary to execute all steps in detail. A full analysis of the possible threats can be skipped. When the vulnerabilities are identified it isn't hard to imagine how these vulnerabilities can be misused. It better to focus on a more extensive analysis of the possible vulnerabilities.

9.6 Summary

In this chapter I have discussed multiple elements of the privacy risk assessment methodology. An mayor contribution to the privacy risk assessment was the definition of architectural views. First of all a view with in the center a business process related to multiple elements in the business and application layer. This view clearly shows the vulnerabilities that are exposed in relation to certain business processes. The second view with meaningful insights is the one where these vulnerabilities are mitigated by showing which control measure reduce the impact of the vulnerabilities.

The definition of the vulnerabilities however, together with the threats, was difficult. Identifying the vulnerabilities is an important but difficult task. The gathering of the vulnerabilities is limited to interviews and general vulnerabilities when there are no logs of vulnerabilities that have been an issue in the past. Furthermore, it can be a challenge to correctly define a vulnerability and making the correct distinction between a vulnerability and a threat.

An important element of the privacy risk assessment methodology is the incorporation of the privacy rules and regulations. These are mapped on security policies and principles in the architecture domain. By doing so the origin of the control measures can be made visible in enterprise architecture views. These rules and regulations are an important driver behind the execution of the analysis and the implementation of the control measures.

The methodology as defined by Jonkers and Quartel (2016) lent himself well to be adjusted to the scope of this research. This methodology has some powerful features. It clearly followed the risk taxonomy, incorporated the mitigating of the risks and came with a mapping between the steps and ArchiMate elements. A point of improvement may be the excessive number of steps. Not all steps are as useful in practice as they may seem in theory. When executing the methodology in practice some step may be skipped.

10 Conclusion

10.1 Answering research questions

The research started with a literature research to set some groundwork and to answer some of the research questions. The first research question to answer was:

Which privacy regulation(s) do organizations in the health care industry have to comply to?

First of all there is a national health care system. The financing of the Dutch public health care system is regulated by four laws, each of which cover a different set of health care. The ZVW is the main health care act cover all basic health care. WLZ takes care who are chronically ill, the WMO covers social support and the is a health care act for those who young and need special treatment.

Secondly, there are privacy rules and regulations. Almost all organizations in the health care industry process personal information of their customers in order to fulfill their jobs. The collecting and processing of personal information is regulated. Until recently the WBP protected the personal information of individuals, currently the AVG or GDPR has replaced this law. These rules and regulations are needed to protect someone's privacy. The processing of personal information is limited by many restriction. The processor has multiple responsibilities regarding the safe and careful processing of personal information and the concerned individual has rights to check and revise his personal information.

Not being compliant with regulations can lead to fines, reputation and financial losses. Especially regarding the GDPR the fines can be pretty high, as high as 4% of the annual income. So it is at least an financial interest to become compliant with these regulations. Regulatory compliance and risk management teach us how organizations van become compliance.

Can we define an element of a reference architecture to help organizations in the medical supplies lending industry to be compliant with privacy rules and regulations?

A reference architecture is a general architecture used to define a group of solution architectures often in the same domain. These reference architectures are often based on best practices and are therefore used by organizations in the same domain to design or redesign their own architecture. An enterprise architecture can be such an architecture. An enterprise architecture

is a blueprint of an organization including both business and technology. (*The Open Group* 2017) is a well-known framework used to design enterprise architecture while *ArchiMate*® 2017 is a well-known enterprise architecture modeling language. They are often used together to define and describe enterprise architectures.

A reference architecture can include many elements. For the health care domain the challenges regarding being compliant with privacy rules and regulations is a primary interest. So there must be an element focusing on mitigating the risk of losing personal information of clients and therefore a risk of receiving a fine. The proposed privacy risks and personal information management methodology is such an element. It is based on a proven risk assessment methodology and focuses on mitigating risks in relation to privacy. It incorporates the applicable privacy regulations and helps organizations to assess their current processes. The result of the methodology is a set of control measures that should be implement to reduce the possibility of a loss event.

How does the defined element perform?

The designed methodology was validated at Welzorg. The application of the methodology resulted in multiple interesting results.

The basic request handling process was evaluated. The evaluation resulted in the discovery of vulnerabilities in relation to the privacy. Personal information was processed on printed forms, information was available for employees that did not need the information and there was a lack of privacy awareness among employees. Based on further analysis of these vulnerabilities finally some control measures were proposed to mitigate the risk associated with the vulnerabilities.

For health care organizations in general the designed methodology will help to evaluate those parts of the organization that deal with personal client information. By systematically evaluating the business processes and applications vulnerabilities can be detected before they are exploited and lead to a loss of personal information. The detailed description of how to execute a privacy risk assessment can help other organizations to execute such an assessment. The mapping of privacy regulations on enterprise architecture elements will also be helpful for other organizations and should therefore be part of a reference architecture for the health care industry.

10.2 Limitations and future research

The performed research has limitations and that's one reason why future research is recommended. In this section the limitations of the executed research are highlighted as well as the possible research directions of future studies.

The validation of the developed methodology was only executed at one organization. For the methodology to become mature validation is needed at multiple organizations. This is also a requirement before this methodology can become a mature element of a reference architecture.

The current design heavily leans on the way vulnerabilities are being addressed. Once the vulnerabilities are identified the other steps of the methodology follow one another. The identification of the vulnerabilities is a weak spot of the methodology. There is limited input available to properly identify applicable vulnerabilities while there are so many possible vulnerabilities.

10.2.1 Towards a reference architecture

An important step towards a reference architecture for the health care industry will be the generalization of the designed methodology. The designed methodology has to be validated at multiple organizations and adjusted after each validation loop.

Future research should also focus on multiple shared processes between these organizations. The process evaluated at Welzorg, the basic request handling, is one of many health organization specific processes.

One of the most important elements of the methodology is the mapping of the privacy rules and regulations on the enterprise architecture domain. Although many parts of the privacy laws were included in this mapping it is worth investigating how to include more elements of these regulations. With the introduction of the GDPR many new restrictions arise and the full impact of this new law becomes more and more visible.

10.3 Recommendation for Welzorg

To validate the designed methodology a case study was executed at Welzorg. Besides the validation of the methodology the case study also resulted in insight at Welzorg. The output of this validation process could also be used to make some recommendations towards Welzorg. Recommendation regarding the processing of personal information in order to become compliant with privacy rules and regulations. In this section I will summarize these recommendations.

To be able to control and monitor who has access to which data Welzorg should implement a centralized authorization and authentication system. One of the key elements of GRPD is to give as little access to personal information as possible. Although some personal information is needed in business processes to be able to execute them, the information should only be accessible by those who execute these processes. In an organization like Welzorg many

different IT systems so accidentally providing someone access to the wrong system can already compromise personal information. This can be prevented by administrating the access to these systems in a central place.

The ability to apply tight authentication and authorization on information shared on paper is almost impossible. It is therefore important to reduce the use of paper to share personal information as much as possible. Especially when the paper is shared outside the organization where there is no longer control over the environment. Unfortunately it is not always possible to fully eliminate the usage of paper due to legal requirements or agreements with third parties. But when this is the case the information that is shared should be the bare minimum needed to fulfill these processes.

But in the end the employees are still the weakest link since their behavior can't be fully controlled. Although most employees don't even want to do any kind of harm unintended action can still cause damage. A well implemented authorization and authentication system can reduce the amount of damage such an action can cause. But to be able to perform their tasks employees need access to some personal information. Awareness among the employees that have access to personal information is an important control measure to protect personal information. People have a natural tendency to conform to comply to regulations. Therefore it is both useful and necessary to inform the employees about the sensitivity of the personal information they are dealing with.

To become compliant with (new) privacy regulations the implementation of these tree recommendations are step in the right direction for Welzorg.

Bibliography

Angelov, Samuil, Paul Grefen, and Danny Greefhorst (2012). „A Framework for Analysis and Design of Software Reference Architectures“. In: *Information and Software Technology* 54.4, pp. 417–431.

ArchiMate® (2017). URL: http://www.archimate.nl/ (visited on June 22, 2017).

Architectuur AORTA (2016). URL: https://www.vzvz.nl/uploaded/FILES/htmlcontent/AORTA2015v6.14/AORTA_Arch_Architectuur_AORTA.pdf (visited on July 5, 2017).

Asser Courant (2016). *Gemeente Assen Verstrekt BSN Met Geboortedatum WMO-Cliënten Aan Derden. 'Dit Mag Wettelijk Niet, We Gaan Er Direct Mee Aan de Slag'*. URL: https://www.assercourant.nl/algemeen/450821/gemeente-assen-verstrekt-bsn-met-geboortedatum-wmo-cli-nten-aan-derden-dit-mag-wettelijk-niet-we-gaan-er-direct-mee-aan-de-slag.html (visited on Dec. 18, 2017).

Autoriteit Persoonsgegevens (2017). URL: https://autoriteitpersoonsgegevens.nl/ (visited on Oct. 3, 2017).

Band, Iver, Wilco Engelsman, Christophe Feltus, et al. (2015). *Modeling Enterprise Risk Management and Security with the ArchiMate®*.

Bishop, M. (2007). „About Penetration Testing“. In: *IEEE Security Privacy* 5.6, pp. 84–87. DOI: 10.1109/MSP.2007.159.

BiZZdesign (2017). *ERSM Getting Started Guide*.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat (2010). „Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness“. In: *MIS Quarterly* 34.3, pp. 523–548. JSTOR: 25750690.

Casey, Timothy (2007). „Threat Agent Library Helps Identify Information Security Risks“. In: *Intel White Paper, September*.

Cloutier, Robert, Gerrit Muller, Dinesh Verma, et al. (2009). „The Concept of Reference Architectures“. In: *Systems Engineering*, pp. 14–27.

Deiters, Constanze, Patrick Dohrmann, Sebastian Herold, and Andreas Rausch (2009). „Rule-Based Architectural Compliance Checks for Enterprise Architecture Management“. In: IEEE, pp. 183–192.

Fattah, Ahmed (2009). „Enterprise Reference Architecture“. In: *22nd Enterprise Architecture Practitioners Conference, London, UK*.

Fried, Charles (1968). „Privacy“. In: *The Yale Law Journal* 77.3, p. 475. DOI: 10.2307/794941. JSTOR: 794941?origin=crossref.

GEMMA (2017). URL: http://www.gemmaonline.nl/ (visited on June 26, 2017).

General Data Protection Regulation (2016). URL: http://data.europa.eu/eli/reg/2016/679/oj (visited on May 30, 2017).

Greefhorst, D, P Grefen, E Saaman, P Bergman, and W Van Beek (2009). „Herbruikbare Architectuur - Een Definitie van Referentiearchitectuur". In: *Informatie*, pp. 8–14.

Greve, R. J. (2016). *The Use of Dutch Governmental Reference Architecture in the Public/Private Healthcare Domain*.

Howard, Philip (2013). *Master Data Management*.

Hughes, R.L. David (2015). „Two Concepts of Privacy". In: *Computer Law & Security Review* 31.4, pp. 527–537.

Humphreys, Edward (2008). „Information Security Management Standards: Compliance, Governance and Risk Management". In: *information security technical report* 13.4, pp. 247–255.

Iacob, M. E., D. Jonkers, H. Quartel, H. Franken, and H. van den Berg (2012a). *Delivering Enterprise Architecture with TOGAF® and ARCHIMATE®*. Enschede: BIZZdesign.

Iacob, Maria-Eugenia, Dick Quartel, and Henk Jonkers (2012b). „Capturing Business Strategy and Value in Enterprise Architecture to Support Portfolio Valuation". In: IEEE, pp. 11–20.

Ionita, Dan (2013). *Current Established Risk Assessment Methodologies and Tools*.

ISO (2011). „ISO/IEC 42010 Systems and Software Engineering-Recommended Practice for Architectural Description of Software-Intensive Systems". In: *ISO/IEC* 42010.

ISO/IEC 27001 (2013). *Information Technology — Security Techniques — Information Security Management Systems — Requirements*.

ISO/IEC 27002 (2013). *Information Technology — Security Techniques — Code of Practice for Information Security Control*.

ISO/IEC 27799 (2016). *Health Informatics — Information Security Management in Health Using ISO/IEC 27002*.

Jeugdwet (2014). URL: http://wetten.overheid.nl/BWBR0034925 (visited on June 28, 2017).

Jonkers, Henk (2014). *Enterprise Architecture-Based Risk Assessment with ArchiMate*. URL: http://blog.bizzdesign.com/enterprise-architecture-based-risk-assessment-with-archimate (visited on Nov. 1, 2017).

Jonkers, Henk and Dick A. C. Quartel (2016). „Enterprise Architecture-Based Risk and Security Modelling and Analysis". In: *Graphical Models for Security: Third International Workshop, GraMSec 2016, Lisbon, Portugal, June 27, 2016, Revised Selected Papers*. Ed. by Barbara Kordy, Mathias Ekstedt, and Dong Seong Kim. Cham: Springer International Publishing, pp. 94–101.

KING (2017). URL: http://kinggemeenten.nl/ (visited on June 27, 2017).

Kosutic, Dejan (2017). *Free List of Information Security Threats and Vulnerabilities*. URL: https://advisera.com/27001academy/knowledgebase/threats-vulnerabilities/ (visited on Nov. 30, 2017).

Mayer, Nicolas, Eric Grandry, Christophe Feltus, and Elio Goettelmann (2015). „Towards the ENTRI Framework: Security Risk Management Enhanced by the Use of Enterprise Architectures." In: *CAiSE Workshops*, pp. 459–469.

Ministerie van Volksgezondheid, Welzijn en Sport (2016). *Het Nederlandse zorgstelsel*.

Nakagawa, Elisa Yumi and José Carlos Maldonado (2008). „Reference Architecture Knowledge Representation: An Experience“. In: *Proceedings of the 3rd International Workshop on Sharing and Reusing Architectural Knowledge*. SHARK '08. New York, NY, USA: ACM, pp. 51–54.

NEN 7510 (2011). *Medische Informatica - Informatiebeveiliging in de Zorg*. URL: https://www.werkenmetnen7510.nl/publicaties/nen-7510-2011 (visited on Oct. 11, 2017).

NORA Online (2017). URL: https://www.noraonline.nl/wiki/NORA_online (visited on Dec. 5, 2017).

NOREA (0011–2015). *Handreiking Privacy Impact Assessment*.

NZa (2017). *Marktscan Zorgverzekeringsmarkt 2017*.

Peffers, Ken, Tuure Tuunanen, Marcus A. Rothenberger, and Samir Chatterjee (2007). „A Design Science Research Methodology for Information Systems Research“. In: *Journal of Management Information Systems* 24.3, pp. 45–77.

Racz, Nicolas, Edgar Weippl, and Andreas Seufert (2010). „A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC)“. In: *Communications and Multimedia Security*. Springer, pp. 106–117.

Sadiq, Shazia and Guido Governatori (2010). „Managing Regulatory Compliance in Business Processes“. In: *Handbook on Business Process Management 2*. Ed. by Jan vom Brocke and Michael Rosemann. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 159–175. DOI: 10.1007/978-3-642-01982-1_8.

Sadiq, Shazia, Guido Governatori, and Kioumars Namiri (2007). „Modeling Control Objectives for Business Process Compliance“. In: *Business Process Management*. Ed. by Gustavo Alonso, Peter Dadam, and Michael Rosemann. Vol. 4714. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 149–164. DOI: 10.1007/978-3-540-75183-0_12.

Solove, Daniel J. (2006). „A Taxonomy of Privacy“. In: *University of Pennsylvania Law Review* 154, p. 477.

– (2008). *Understanding Privacy*. SSRN Scholarly Paper ID 1127888. Rochester, NY: Social Science Research Network.

Sowa, J. F. and J. A. Zachman (1992). „Extending and Formalizing the Framework for Information Systems Architecture“. In: *IBM Systems Journal* 31.3, pp. 590–616.

Sutinen, Jon G. and K. Kuperan (1999). „A Socio-Economic Theory of Regulatory Compliance“. In: *International Journal of Social Economics* 26 (1/2/3), pp. 174–193. DOI: 10.1108/03068299910229569.

Syed Abdullah, Norris, Shazia Sadiq, and Marta Indulska (2010). „Emerging Challenges in Information Systems Research for Regulatory Compliance Management“. In: *Advanced Information Systems Engineering: 22nd International Conference, CAiSE 2010, Hammamet, Tunisia, June 7-9, 2010. Proceedings*. Ed. by Barbara Pernici. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 251–265. DOI: 10.1007/978-3-642-13094-6_21.

The Open Group (2011). *The Open Group Architecture Framework® Version 9.1*. Van Haren. 695 pp.

– (2016). *ArchiMate® 3.0 Specificaiton*. Van Haren. 184 pp.

The Open Group (2017). URL: http://www.opengroup.org/ (visited on June 22, 2017).

VECOZO (2017). URL: https://www.vecozo.nl/ (visited on Oct. 11, 2017).

Vektis (2017). URL: https://www.vektis.nl (visited on Oct. 11, 2017).

Vicente, Pedro and Miguel Mira da Silva (2011). „A Conceptual Model for Integrated Governance, Risk and Compliance“. In: *Advanced Information Systems Engineering*. Ed. by Haralambos Mouratidis and Colette Rolland. Red. by David Hutchison, Takeo Kanade, Josef Kittler, et al. Vol. 6741. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 199–213. DOI: 10.1007/978-3-642-21640-4_16.

Vicente, Pedro, Nicolas Racz, and Miguel Mira da Silva (2011). *Towards a Reference Model for Integrated Governance, Risk and Compliance*.

VNG (2017). URL: https://vng.nl/ (visited on Oct. 11, 2017).

Welzorg (2017). URL: http://www.welzorg.nl (visited on May 24, 2017).

Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (2017). URL: http://wetten.overheid.nl/BWBR0023864/2017-07-01 (visited on Oct. 3, 2017).

Wet algemene bepalingen burgerservicenummer (2007). URL: http://wetten.overheid.nl/BWBR0022428 (visited on May 30, 2017).

Wet bescherming persoonsgegevens (2000). URL: http://wetten.overheid.nl/BWBR0011468 (visited on May 24, 2017).

Wet langdurige zorg (2014). URL: http://wetten.overheid.nl/BWBR0035917 (visited on May 30, 2017).

Wet maatschappelijke ondersteuning 2015 (2014). URL: http://wetten.overheid.nl/BWBR0035362 (visited on May 30, 2017).

Zorgverzekeringswet (2005). URL: http://wetten.overheid.nl/BWBR0018450 (visited on May 30, 2017).

List of Abbreviations

BSN Dutch national identification number *(Burgerservicenummer)*

DPO Data Protection Officer

ERSM Enterprise Risk and Security Management

EU European Union

GDPR General Data Protection Regulation

GRC Governance Risk and Compliance

IS Information Systems

KDU Short Term Lease *(Kort Durende Uitleen)*

KING Knowledge Institute for Dutch Municipalities *(Kennisinstituut Nederlandse Gemeenten)*

NORA Dutch Government Reference Architecture *(Nederlandse Overheid Referentie Architectuur)*

PIA Privacy Impact Assessment

VNG Association for Dutch Municipalities *(Vereniging Nederlandse Gemeenten)*

WBP Dutch Data Protection Act *(Wet bescherming persoonsgegevens)*

WLZ Dutch Long-term Care Act *(Wet langdurige zorg)*

WMO Dutch Social Support Act *(Wet maatchappelijke ondersteunding)*

ZVW Dutch Health Care Act *(Zorgverzekeringswet)*