Information Security in the Dutch Health Insurance Industry

Analyzing the impact of the Dutch Data Protection Act and the reformed European Privacy Act at Dutch health insurers

Author
Tim J.F. Bus
Master Industrial Engineering & Management,
Specialization IT & Management

Reference manager: Zotero, style APA 6th edition

Supervisors University of Twente
Prof. Dr. J. van Hillegersberg
Prof. Dr. M. Junger

Supervisors ConQuaestor
Erik Janse
Luc Idzinga

Author
T.J.F. Bus
Student Nr.: s0209171
University of Twente

Master program
Industrial Engineering & Management

Specialization
IT & Management

Graduation Date
T.b.a.

Graduation Committee
1st Supervisor: Prof. Dr. J. van Hillegersberg
University of Twente

2nd Supervisor: Prof. Dr. M. Junger
University of Twente

External Supervisor: E. Janse
ConQuaestor

External Supervisor: L. Idzinga
ConQuaestor

University of Twente.
Drienerlolaan 5
7522 NB, Enschede
The Netherlands

ConQuaestor
Orteliuslaan 871
3528 BE, Utrecht
The Netherlands

Management Summary

In this thesis we present a research on Information Security at Dutch health insurers, with the purpose of giving insight in the current maturity, and providing a guide on quick-wins for Information Security improvements. This research is sparked by 1) research project of the Dutch National Bank on the state of Information Security at Dutch financial institutions, 2) the relevance of Information Security in light of the new European privacy regulations, and 3) the necessity of Information Security for health insurers because of the significant amounts of privacy sensitive health data they collect.

In order to develop an analytical framework for the assessment of Information Security maturity at health insurers we have firstly created an insight in the European General Data Protection Regulation in comparison with the Dutch Data Protection Act. Secondly a literature study of both scientific and practice-oriented research was conducted. For the framework we have taken ISACA's Business Model for Information Security as a basis, and combined it with insights from COBIT 5 and ISO 27000.

After the literature study the research population, CIO's and Security Officers at health insurers, was been contacted for an interview of about one hour, and the filling of the analytical framework. These interviews and the filling of the framework had the purpose of testing and verifying the analytical framework. However, because only three out of nine organizations responded to the interview request this data collection step yielded too little data too analyze with SPSS. Therefore we have not been able to statistically verify the findings from literature and the analytical framework.

We conclude from this research that the since about the start of the DNB research on Information Security in 2010 the Information Security function has been significantly professionalized to maturity level 3. The general attitude among insurers is that keeping health data safe is rooted in their nature. With the little data we collected we can make a conservative estimate that the analytical framework is to a large degree correct and usable to analyze health insurers. We find that the main technological measures for Information Security, such as network compartmentalization, firewalls, Identity and Access Management, have been developed by all interviewed organizations to at least a sufficient degree. However, for further maturity development the human factor plays a significant role. Therefore, all insurers are currently executing or developing security awareness programs to increase the awareness of Information Security threats, mainly among non-IT personnel.

With regard to the analytical framework we developed we have too little data to be able to verify and sharpen the framework. However, from the one organization that filled the framework we can make a safe statement that the basis of the framework is correct and applicable.

In addition to the findings and recommendations for insurers we make several suggestions for the DNB and the European Commission. To the DNB we suggest to renew the Information Security research, and present an insight in the current state of Information Security at financial institutions. This may increase trust among consumers, and motivate organizations to follow the improvement of Information Security. To the European Commission we suggest to distinguish companies based on the purpose of data processing, i.e. differentiate between companies that process data for their own benefit and companies that process data for the benefit of the client. Finally, to the CBP and European supervisors we suggest to provide clear and practical guidelines that provide a guide to compliance, so that it is clear what the regulator and supervisor expect from the company.

Preface

First of all I want to thank my supervisors at ConQuaestor and the University of Twente for supervising my work and sharing their experience with me. They have left much room for me, while pushing me in the right direction when I needed it. Especially I want to thank my supervisor Luc Idzinga for always being there when there when I needed him. I am very grateful for the look behind the scenes at many of the health insurers into such a delicate and precarious matter as Information Security. Besides my supervisors and the people I have interviewed I want to thank Judith Vieberink for her support regarding privacy laws. I can imagine that it takes even more bravery to do that when they know that the situation isn't all that bright and shiny at their company. In addition I want to thank my parents, friends and family, especially my nephew Björn, for supporting, helping, and sometimes even distracting me.

The research process in this thesis was quite hard for me since I didn't have all that much experience with information security and privacy regulations. In addition, the health insurance branch was difficult to approach through my existing contacts or my supervisors. Besides, I have had to revise and sharpen the focus several times because either the subject was too broad or the diversity in research population was too great. However, the whole master thesis project is both a knowledge application and a learning stage in the studies and I have definitely become much wiser throughout the whole process.

Tim Bus

Table of Contents

1. Introduction

In this research proposal I will set out a research on the current status of information security at Dutch health insurers, in order to develop a framework that can help assess and improve the level of information security. This research direction is derived from three main sources that highlight the need for a proper information security function. Firstly, the results of a periodic research by the De Nederlandsche Bank (DNB), the Dutch central bank, indicates that information security (InfoSec) at many Dutch financial institutions is not at an appropriate level. A 2011 analysis by DNB concluded that 85% of the financial institutions in The Netherlands, including health insurers, does not take appropriate security measures to be able to attend a sufficiently high level of InfoSec in relation to the sensitivity of the (personal) data that the institutions store (Baveco & Bikker, 2011). For healthcare insurers the activity of InfoSec is essential since they handle highly sensitive personal data, including medical information that should be kept secure and genuine, while it should also be readily available for healthcare providers.

Secondly, numerous research institutes that annually research the occurrence of data breaches, including the Ponemon Institute (2013), Symantec and Verizon (2013, 2014), point out that data breaches are increasing in number and in impact.

Thirdly, the European Commission is preparing an update of the European privacy regulations that will pose a great challenge for all organizations that process privacy sensitive personal data. In the new privacy directive both the required level of information security and the fine for incompliance will significantly increase to a degree that is possibly threatening for the continuity of institutions that process personal data.

However, despite all the sources that give insight in the current state or the necessity of InfoSec there is little (sector specific) insight in the sources of non-compliance/non-conformance. As such, there is not much practical insight for organizations into how they can quickly and sustainably improve their Information Security state/maturity level.

In this introductory chapter the main line and context of this research are set out by giving a short introduction to the field of InfoSec and the Dutch financial industry on the basis of which the problem statement, research questions and research approach are presented. Hereafter the current situation regarding the Dutch health insurance sector and InfoSec will be considered and connected to streams in scientific and practical research.

1.1. Context and scope

In order to provide the context and scope for this research a brief overview of three central themes will be given, which consist of:

1. the Dutch health insurance sector;
2. information security & privacy, and;
3. European privacy regulations.

1.1.1. Dutch Health Insurance Sector

To start, we first demarcate the scope of this research. In this research the focus is exclusively on health insurers and their position in relation to regulators and their customers, which is illustrated in the simple but adequate visual overview of the Financial Services Industry (FSI) in Figure 1. The research population thus includes all health insurers active in the Dutch health insurance sector.

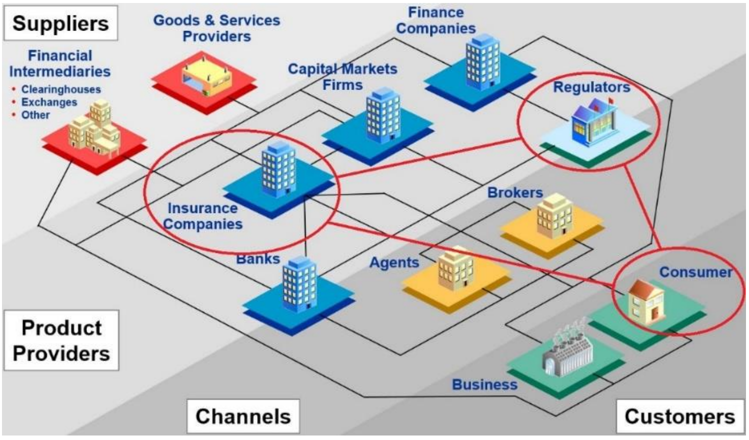


Figure 1: Overview of the financial services industry, focus on health insurers and related entities (adapted from (van Hillegersberg, 2013))

Health insurers in The Netherlands are subject to several Dutch and European regulatory bodies that focus on different aspects of their activities. The most important and most relevant are De Nederlandsche Bank, Nederlandse Zorgautoriteit (NZa), and College Bescherming Persoonsgegevens (CBP).

The DNB fulfills the role of supervisor on the genuine and honest execution of the insurance activities of a health insurer, but also focuses on the threats to continuity such as financial stability and information security (or lack thereof). The NZa, the Dutch healthcare authority, as a healthcare supervisor mainly focuses on the compliance with Dutch healthcare regulations. Finally, the CBP is the Dutch supervisor that focuses on compliance with the Dutch and European privacy regulations that apply to organizations that process personal information.

The Dutch health insurance sector is discussed in more detail in chapter 2.

1.1.2. Information Security & Privacy

We take the definition of "information security" from the US Code Title 44 Chapter 35, subchapter III, §3542:

> *"Information security is the protection of information and information systems from unauthorized access, user, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability".*

Information security (InfoSec) is a key activity for health insurers, since they deal with an immense volume of privacy sensitive data. Therefore the focus will be especially on the security of information that can be classified as 'privacy sensitive', or 'personal data', which is defined in article 1 of the Dutch Data Protection Act as:

> *"any information relating to an identified or identifiable natural person"* (Ministerie van Veiligheid en Justitie, 2000)

There are numerous factors recognized in research that influence the state of InfoSec in companies. Most of these factors can be grouped roughly in the elements named in the Business Model for Information Security (BMIS) as illustrated in Figure 2. The BMIS is an ISACA extension of the ICIIP Model developed at the University of Southern California's Institute for Critical Information Infrastructure Protection (ICIIP). The model includes four elements, or nodes, that represent the four concepts organization, process, people and technology, which are connected to each other by branches that represent the mechanisms through which the elements are connected. The four concepts roughly represent the main areas in which Information Security is governed in an organization. Therefore we can use this model to explain deficiencies in InfoSec, suggest specific areas for improvement, and help build a business case for Information Security by highlighting the necessity for the business as a whole.

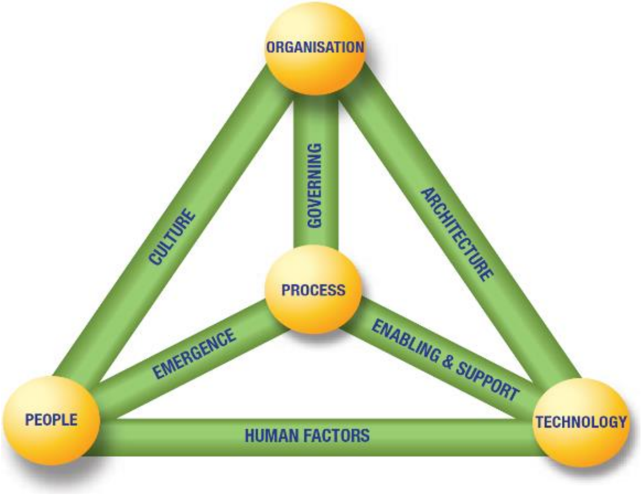


Figure 2: Business Model for Information Security (Kiely & Benzel, 2006), (Roessing & Information Systems Audit and Control

Since this conceptual model includes all the key aspects of InfoSec that are relevant for this research project it will be used as the basic theoretical framework for this research. This model will be further discussed in chapter 4.

1.1.3. Privacy regulations

In the Netherlands the protection of personal data is established in the "Wet Bescherming Persoonsgegevens" (Dutch Personal Data Protection Act, or DPA), which is based on the European data protection directive 95/46/EC of December 1995 and is active since September 2001. The law is governed in The Netherlands by the CBP. The current DPA is mainly a generic norm on the basis of which organizations are expected to implement an adequate InfoSec function. The DPA provides the regulator with limited instruments to enforce organizations to properly secure the personal data, an example is the provision that gives organizations an "obligation to report in case of a data leak", on which stands a maximum penalty of €4.500. It can be argued that with penalties of this small sum, the regulator lacks the proper tools to properly direct information security at the larger organizations.

Partially because of the lack of proper tools and the normative character the current EU directive was deemed outdated by the European Commission, and will be replaced in the forthcoming years by the European *"General Data Protection Regulation"* (GDPR), also called the *European privacy directive*. This directive is intended to replace all current privacy regulations in EU member states. In response to the draft GDPR the Dutch DPA is already be adapted reflect the requirements set in the European GDPR, and will provide the Dutch regulator CBP with numerous new and modified instruments to enforce organizations that process personal data to get their InfoSec right, including:

- a provision that obligates reporting "severe" data leaks within 24 hours of occurrence, with an imposed maximum fine of €450.000 in case of incompliance (NL: Wet Meldplicht Datalekken);
- the delivery of documentation regarding processes in which personal data is processed to the CBP;

- a right for stakeholders (clients) to access, rectify and remove their own personal data;
- that profiling (analyzing and tracking populations) is subject to strict conditions;
- that a “Privacy Impact Analysis” is carried out periodically;
- that new IT projects are developed following a “Privacy by Design” approach;
- that “general” data leaks are reported and solved within a reasonable time-period;
- that a “data protection officer” (NL: Functionaris Gegevensbescherming) is appointed in/by the organization that acts independent and keeps an eye on data protection.

With the replacement of the Dutch DPA by the European GDPR in the forthcoming years, the necessity to be, or become, compliant with privacy regulations will increase significantly. Therefore this research aims to give insight in the current situations and provide a practical guideline to compliance for Dutch health insurers. The European GDPR will be discussed in more detail in chapter 3 of this research.

1.2. Problem identification

1.2.1. Problem statement and research goal

As presented in the introduction the current situation is that only 15% of the Dutch financial enterprises deploy sufficient information security measures to control InfoSec risks. The other 85% deals with significant risks related to:

- *dependence* on external suppliers, *of which little is known with regard to* security arrangements and how suppliers handle sensitive customer information;
- authorizations of employers and IT administrators for access to critical business applications;
- inadequately monitored *IT environments*;
- *inability to keep up with new developments in security needs and measures, and;*
- *inadequate view of i*nformation security*, which is too often* seen as an IT concern *(Baveco & Bikker, 2011)*.

Given description of the context and the results of the DNB Information Security research it is derived that the current state of information security at health insurers is too fragile and should be improved significantly in order to comply with data protection regulations, and to protect the customer and the company as a whole from damage resulting from data leaks and integrity violations. Therefore we derive at the following problem statement:

The percentage of health insurers that complies with all relevant data protection regulations should be increased, especially with the stricter privacy regulations in sight.

The responsibility for the increase in the number of health insurers that complies with data protection regulations lies with the insurers themselves and beyond my sphere of influence. Therefore the main goal in this research is to assess the current state of InfoSec, identify gaps, and suggest a framework that can help insurers identify gaps in order to implement improvements to their InfoSec function.

1.2.2. Research questions

When taking both the problem statement, the BMIS, and the GDPR into account we derive at the following research questions:

How can Dutch health insurers adapt their information- and privacy security practices to prepare for the new, stricter, Dutch and European privacy laws & regulations and achieve full compliance?

1. What is the current status of privacy security at Dutch health insurers?

   a. What measures and abilities do health insurers deploy to maintain privacy security?
      i. Governance regarding security and data management
      ii. Technological security measures
      iii. Non-technological security measures
   b. How many incidents occur yearly in which privacy is breached?
      i. Where do these breaches originate from? (Internal/external)
      ii. What is the impact of these breaches on a company? (Fines, loss of reputation, lawsuits with clients, etc.)
      iii. How do health insurers currently deal with these breaches in practice? (Detection, response, settlement, compliance?)

2. What impact will the new EU and Dutch privacy laws and regulations have on health insurers?
   a. What privacy security measures and abilities are demanded in the new privacy regulations?
   b. What instruments does the law give to regulators?

3. How does the current state of privacy security compare to the situation desired in the privacy laws and regulations?
   a. What gaps with regard to privacy laws and regulations can be perceived from the current situation?
   b. How can health insurers measure/assess their current state of privacy security?

4. How can health insurers practically improve their state of privacy security and become compliant to the privacy regulations?
   a. What improvements can be realized within a short time-frame of 6-12 months?
   b. What improvements can be realized within a longer time-frame of 2-3 years?

1.3. Research methodology

According to the social sciences research principles as presented by Bhattacherjee (2012) this piece of research is explanatory, that is, it is intended to explain phenomena in the real world by examining why and how the problems exist. When we have derived this insight in the real world problems and the situations in which they exist we set out to present a solution guideline targeted at improving the current situation. In this section the data collection methods and the research process through which the research questions were answered will be described and justified.

1.3.1. Data collection

Literature study

As a first approach to this research I have conducted a structured literature study into the Dutch DPA and the consequences of this regulation, Information Security and Organizational Capability Development. In this study the following three types of sources are examined for explaining the current state of InfoSec at health insurers, the current and future data protection regulations, and InfoSec as an organizational capability:

- Scientific literature into various streams of relevant research with the conceptual framework/BMIS as a guideline.
- Regulations and standards documents relevant to the area of information security in financial enterprises as defined in section 3:17 of the Dutch Financial Supervision Act.
- Commercial researches into Information Security and data leaks by Verizon and Deloitte among others;
- Practical management and governance methodologies, e.g. COBIT.

Following the data and knowledge derived from the interviews that followed the literature study a second brief literature research step was conducted in order to explain compliance and maturity problems, and to be able to suggest possible "solutions" for the improvement of the current situation. This study examines the following sources:

- Scientific literature into various streams of relevant research with:
    1. the conceptual framework/BMIS as a guideline, and;
    2. the interview results as a guideline.
- Commercial researches into Information Security and data leaks by Verizon and Deloitte among others;
- Practical management and governance methodologies, e.g. COBIT.

Interviews

As a second data collection step interviews have been conducted with the purpose of qualitatively analyzing the current situation, and the corresponding problems from which the perceived lack of information security results. Firstly, a brief telephonic interview with the writer of the circular at De Nederlandsche Bank was conducted to examine the background of the 2011 circular and DNB's view on the current situation in the health insurance sector. Secondly, a mapping of all relevant health insurers was made in order to identify the research population. Out of the total of nine health insurance companies in the Dutch market eight have been approached for an interview. Interviews were conducted at four companies that responded positively to the request. These four together cover a total market share of >80%. Two companies refused cooperation and two companies did not respond to a request for an interview.

For the interviews the CIO, CISO and/or CSO, and highly placed Information Security Managers were targeted, depending on the function responsible for InfoSec in the organization. The interviews were structured to ensure validity and comparability of answers. Afterwards, the interviews have been summarized, since transcription was not possible, and analyzed in order to sketch the current situation of information security at health insurance companies. To obtain more insight in the sensitive and confidential subject of InfoSec all interviews were processed as anonymous for this research.

In addition to the interviews the health insurers were asked to fill in the analytical framework that resulted for this research, which will be discussed in the following section.

Analytical framework

The analytical framework that results from this research is intended to determine the maturity of personal data security at health insurance organizations. The framework can, as such, be used as a way of data collection through which quantitative data is obtained. The quantitative results can be analyzed with the statistics program SPSS, and in this way results from interviews can be verified and possibly extended when enough filled-in frameworks are obtained from health insurers.

1.3.2. Validation

To ensure the internal validity of the research the interviews are all structured to be able to compare answers and verify the guideline with various health insurance companies and regulatory bodies. In addition, the mechanisms proposed in the guideline will be verified with best-practices and scientific literature. The external validity can be guaranteed by having a sufficiently large research population of health insurers so that errors caused by individual organizations can be filtered out. I aim at visiting all organization, but think that a good minimum target is that visiting 5 to 6 out of 8 would qualify as "sufficient" since we then take a broad range of organizations into account.

1.4. Structure of thesis

In this thesis the following basic structure is kept for the explication of the research. In this chapter the boundaries of this research have been set out, the conceptual framework was presented, and the research methodology was described. In chapter 2, insight in Information Security from practical and scientific research will be given. After that, in the chapters 3 and 4 we will give further insight in the situation with regard to health insurers and the current and future privacy regulations. Based on the knowledge gathered in the first four chapters the analytical framework for the Information Security capability at health insurers will be constructed and presented in chapter 5, while the results of the data collection step and the interviews will be discussed in chapter 6. The conclusion of this research will be given in chapter 7 together with the recommendations and a discussion of the research process, including possible biases that have to be taken into account and directions for future research.

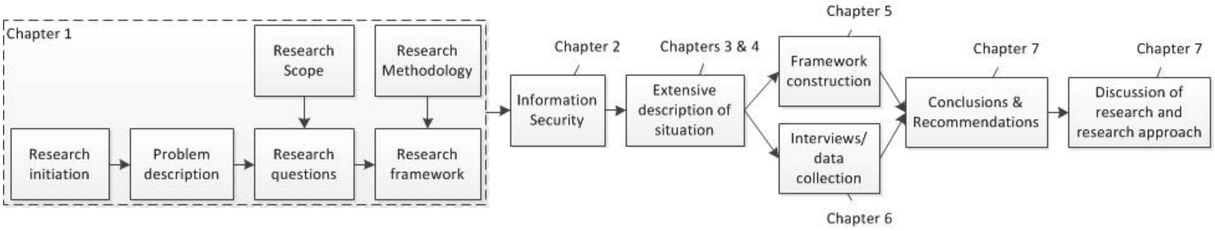


Figure 3: Main structure of this thesis

2. Information Security

In this chapter the current practices in Information Security will be discussed. The structure of this chapter, and consequently also the literature study on Information Security, is outlined in Figure 4. Firstly, a short introduction will be given on Information Security after which the focus will be on the evolution of Information Security and IT in the financial services industry and particularly at insurers. Secondly, an overview will be presented on the main internal and external risks and threats that organizations nowadays face with regard to data breaches, and which are mitigated or minimized through good information security practices. In section 2.3 the main literature study for this piece of research will be set out. This part is subdivided in two sections in which the following subjects will be described:

1. the current practices and standards in Information Security that the health insurers can implement or have implemented;
2. the development and realization of these practices in the organization explained from a change management perspective, and;

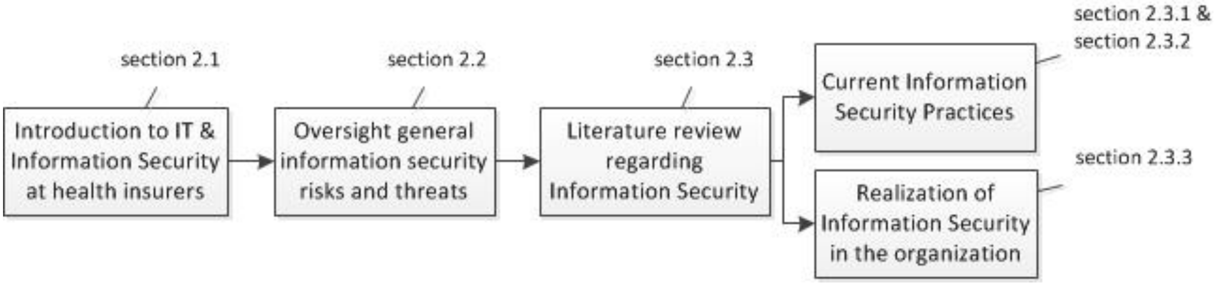
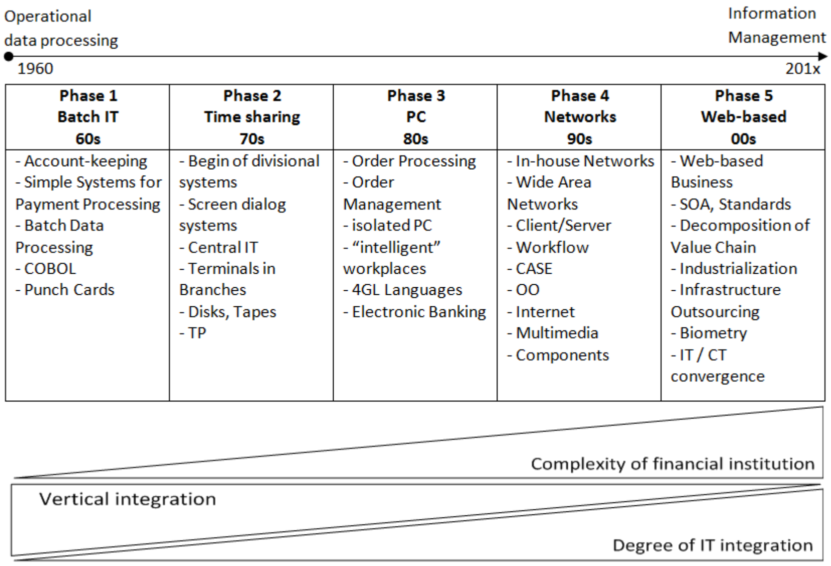

section 2.1
Introduction to IT & Information Security at health insurers
section 2.2
Oversight general information security risks and threats
section 2.3
Literature review regarding Information Security
section 2.3.1 & section 2.3.2
Current Information Security Practices
section 2.3.3
Realization of Information Security in the organization

Figure 4: Structure of chapter 2

2.1. A short introduction on IT and Information Security

The storage, processing, and transfer of information has seen a revolution since the emergence of information technology; digital has replaced analog in practically 99% of data communication and processing in companies from the 1960s on. The revolution is especially significant in the financial services industry, which traditionally is very data intensive. Banks and insurers have, through the years, become IT companies with immense databases as their most valuable assets.

The evolution of the financial services world can be seen in the timeline presented by Moormann & Schmidt, (2006) in Figure 5. The illustration is based on the banking sector, but the change empowered by IT influenced insurers greatly in a comparable way. The change lies mostly in the automation of an increasing number of processes. The use of IT started with the batch processing of data. In the 70s, when IT took a flight and computing capacities increased, the first central and divisional IT systems started to emerge. These were mainly terminals connected to a mainframe for calculations and storage of data. The 80s followed with the introduction of the PC, which brought efficiency gains in administrative tasks while also increasing functionality. Through the connections established between banks, electronic banking started to emerge. In the 90s the internet enabled wide-area networks, which enabled more advanced in-house and external networks in which the terminal connections to mainframes were no longer needed and PC's and servers took over their functionality. In the 2000s, the internet grew and became a common good, and IT developed more potential with the upcoming web-based business and the Service oriented architecture (SOA). (Moormann & Schmidt, 2006)



Phase 1 Batch IT 60s	Phase 2 Time sharing 70s	Phase 3 PC 80s	Phase 4 Networks 90s	Phase 5 Web-based 00s
- Account-keeping - Simple Systems for Payment Processing - Batch Data Processing - COBOL - Punch Cards	- Begin of divisional systems - Screen dialog systems - Central IT - Terminals in Branches - Disks, Tapes - TP	- Order Processing - Order Management - isolated PC - "intelligent" workplaces - 4GL Languages - Electronic Banking	- In-house Networks - Wide Area Networks - Client/Server - Workflow - CASE - OO - Internet - Multimedia - Components	- Web-based Business - SOA, Standards - Decomposition of Value Chain - Industrialization - Infrastructure Outsourcing - Biometry - IT / CT convergence

Figure 5: Timeline of IT in the financial services industry (Moormann & Schmidt, 2006)

With the total use of IT for data processing, transfer and storage, and the growing use of the internet emerged a great vulnerability. Before the IT and the internet era data transfer was slow, processing was manual, and data accumulation occurred literally in data warehouses. Though in this era, information may easily have been stolen, leaked or altered, the InfoSec function had a completely different meaning. There was only a small group of people with access to the data, a guard at the door prevented unauthorized access, and integrity was maintained by strictness and accuracy during processing and through maintaining records. (Moormann & Schmidt, 2006)

Since the emergence of the internet data processing has changed immensely. Sharing with the whole world can be done nearly instant, malicious code can influence integrity of data without anyone noticing, and hackers from outside the organization can work their way in through unnoticed backdoors to steal or alter data. The vast increase in data processing capabilities enabled by information technology has great detrimental effects, including the risk of data breaches, unauthorized data modification, and data theft. As such, the traditionally relatively simple InfoSec function has to develop into a complex organizational capability that is able to fight and repel battles on numerous, and very diverse, fronts to maintain confidentiality, availability and integrity of the data in the organization. (Moormann & Schmidt, 2006)

2.1.1. Information Security in the IT era

In order to protect companies and their customers from fraudsters and hackers, governments around the world have adopted privacy protection laws and regulations. These laws and regulations, such as the EU Privacy Act and Dutch Data Protection Act, prescribe that organizations that process personal data should protect that data. These regulations provide regulators and supervisors with tools, such as fines, to enforce compliance.

Because the risks and consequences of data leaks and cybercrime have increased significantly during recent years, and organizations still lack behind when it comes to security, the European Union and the United States are tightening laws to enforce strict compliance with more radical and influential measures.

However, since the laws and regulations are often abstract there is little guidance on how an organization can, or should approach InfoSec. Fortunately, there are numerous international fora, organizations and consortia that have developed standards, approaches, guidelines and measures for organizations to follow.

The International Organization for Standardization (ISO) has presented the ISO/IEC 27000 standard for information security management systems, while the Information Systems Audit and Control Association (ISACA) has taken InfoSec into account in its governance and management framework COBIT. In addition, in the Information Security Forum (ISF) organizations share experiences, and develop best- and good-practices regarding Information Security.

2.2. General information security risks

As mentioned, with the evolution of IT there has been a significant increase in the exposure of (private) data sources, which poses great risks for organizations that process large quantities of (personal) data. Violation of the confidentiality, integrity and availability of a data source may cause disruption of processes, damage to reputation, lawsuits, imposition of fines, and indirect and direct financial losses. These consequences may, in turn, have a significant influence on the continuity of an organization.

Although a risk can never be fully mitigated, a company that processes or stores data should effectively execute countermeasures to mitigate and minimize risks and their impacts to minimum. As mentioned, the specific risks that may result in data breaches are quite diverse in form, origin and impact. It follows from both the Verizon Data Breach Investigations Reports of 2013 and 2014 and the Ponemon Institute’s 2013 Cost of Data Breach study that often the main causes of InfoSec related incidents lie in human errors and (unpatched) technical vulnerabilities (Figure 6). The origins of these problems, however, can often be found on higher levels, such as in inaccurate governance, lacking security awareness, and lack of top management attention for InfoSec. (Verizon, 2013), (Verizon, 2014), (Ponemon Institute, 2013)

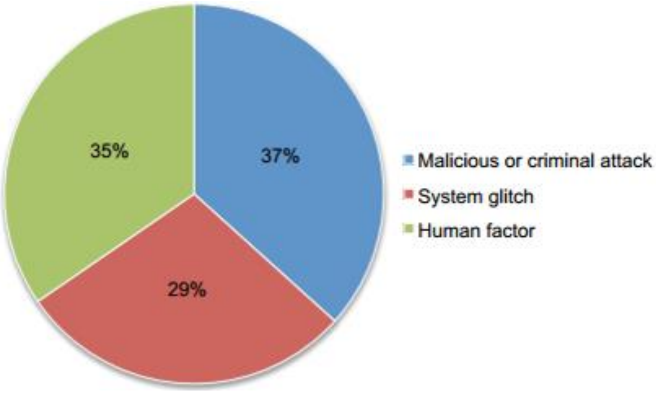


Figure 6: Distribution of a benchmark sample (n=277) by root cause of data breach (Ponemon Institute, 2013, p. 7)

In the following section a selection of the most common internal and external sources data breaches/leaks will be discussed. The sources of these lists of risks are the Verizon 2013 and 2014 Data Breach Investigation Reports, the DNB 2013 and 2014 Supervisory Themes reports, and the interviews with insurers that will be discussed later on. (De Nederlandsche Bank, 2013), (Verizon, 2013), (De Nederlandsche Bank, 2014a), (Verizon, 2014)

2.2.1. Risks to Information Security

Threats to information security can, on the basis of the source from which it originates, be divided in internal and external. Depending on the perimeter set by governance, third-party partners can be both internal and external, albeit this may also depend on the internal sensitivity classification of the data. Data sources can be threatened in one or more aspects of the Confidentiality, Integrity & Availability (CIA) principle, for example a DDOS attack might only threaten (direct) availability while the existence and emergence of Shadow IT, self-made IT applications that emerge in processes and stay under the organizational “radar”, may pose a threat to both confidentiality and integrity.

Internal and external Information Security risks

Information Security risks can be divided, but not mutually exclusive in two bins. Internal risks and external risks. Internal InfoSec risks emerge from inside the company or the company’s perimeter, for example when a group of regular salespersons has excessive rights, or even administrator rights, on a key IT application. On the other hand, external InfoSec risks emerge from an external source to the company, for example in the form of hackers that attack a web application and hereby obtain or influence customer data (confidentiality, integrity) or hijack the web application for a period of time (availability).

A list of several common risks to security and privacy can be found in Table 1.

Table 1: Internal and external security risks (Verizon, 2014), (ENISA, 2013), (Ponemon Institute, 2013)

Vulnerability/risk	Source example	Influence on CIA aspects
Malicious or vulnerable code	- Miscellaneous errors - Zero-day vulnerabilities	- Confidentiality - Integrity - Availability
Human errors	- Ignorance of procedure - Protocol/process error - Form fill mistake (typing error) - Social engineering/phishing	- Confidentiality - Integrity - Availability
Architectural complexity	- Legacy - Many vendors/applications/middleware - Lack of oversight in location of data	- Confidentiality - Integrity
Illegal access (not equal to hacking may not involve a system breach)	- Lacking/inaccurate roles in Role-based Access Control - Lacking access restriction measures (e.g. smart-card door locks, access gates)	- Confidentiality - Integrity
Incautious disposal of information sources (e.g. e-waste, paper)	- PC’s with classified information not disposed of properly - Information on USB-sticks not deleted properly - Paper information sources not shredded	- Confidentiality - Integrity
Shadow IT	- Unapproved applications or changes to applications used in processes - Workarounds for obstructive security created by personnel	- Confidentiality - Integrity
Lacking IT life-cycle management	- Inaccurate disposal of servers, PC’s and digital information carriers (e.g. USB-drives) - Presence of hardware with unsupported Operating Systems (e.g. Microsoft Windows XP or Windows Server 2003) or applications in critical or vulnerable IT systems - Inaccurate tracking of hardware in organization (e.g. what laptops do we have, who has one, etc.) - Inaccurate patching procedures, servers not patched in time	- Confidentiality - Integrity - Availability
Lacking release management	- Changes in applications or processes not documented properly before release	- Confidentiality - Integrity

	- Changes in applications or processes not approved properly before release - Change not audited/tested before release	- Availability
Inaccurate third-party security	- Lack of control over party - Inaccurate contractual agreements - Lacking security measures at third-party	- Confidentiality - Integrity - Availability
Physical theft or loss of a data source/carrier, e.g. laptop, smartphone, paper, and USB-stick	- Awareness of employee - Bad luck	- Confidentiality - Integrity
Hacking	- DDos (technically seen not hacking) - Web Application attacks - Identity theft - Ransomware	- Confidentiality - Integrity - Availability
Crimeware/malware	- Key loggers - Trojan horses - Viruses - Ransomware	- Confidentiality - Integrity - Availability
Social engineering	- Phishing - Advanced Persistent Threats	- Confidentiality - Integrity - Availability

A (partial) base for the risks named in the table above may be an inaccurate, or inaccurately executed, security policy. Daniel Bradley (2003) identifies the following five problems that obstruct an effective security management policy:

- The policy divide, a divide between establishment of enterprise security policy and its enforcement. Such as misunderstanding between management and technical employees.
- Reproducibility of security management depends on the specific work skills to deal with security problem.
- Consistency is hard to ensure between the configurations of devices because of different technology domains.
- Coverage of all aspects. In addition to the huge effort needed to initially configure the policy, it also requires constant maintenance to include newly arising aspects.
- Presently systems are proprietary and inflexible due to this proprietary nature. Due to high license fees, and support contracts, it is very difficult to comply with new security requirement.

Based on these five problems it can be concluded that the security policy requires reviewing, monitoring, and careful revision, since the security policy is a foundation and core part of security management.

2.3. Information Security Frameworks and Best practices

In this section the literature review with regard to Information Security and the development of an InfoSec capability at Dutch health insurers will be presented through the discussion of several important frameworks. Firstly, we will return to the BMIS model as the central conceptual framework in this research. In the second section, three common and important standards/frameworks for InfoSec insurers will be discussed. After that a side-step is made, and the focus will be on to the way in which InfoSec practices can be realized in the organization from a change management perspective.

2.3.1. BMIS

As mentioned in the introduction of this research I have taken the Business Model for Information Security (BMIS) as a central framework for this research. In the documentation of the BMIS the publisher, ISACA (2009), argues that the traditional reactive approach provides a very narrow view of InfoSec in the organization, strictly from the side of the IT department. This view does not sufficiently take the business side, and the organization as a whole, into account, which, on turn, causes the emergence of ineffective, e.g. damagingly inaccurate or otherwise overprotective, measures and controls for InfoSec. The BMIS, on the other hand, is based on the systems thinking approach, which means that the organization is seen as a system that "is an organized collection of parts that are highly integrated to accomplish an overall goal" (ISACA, 2009, p. 10). This approach provides a broader framework of InfoSec in the organization, and puts InfoSec measures and controls more into perspective in the organization. Taking into account the requirements of, and impacts on the business enables the more effective design and implementation of measures.

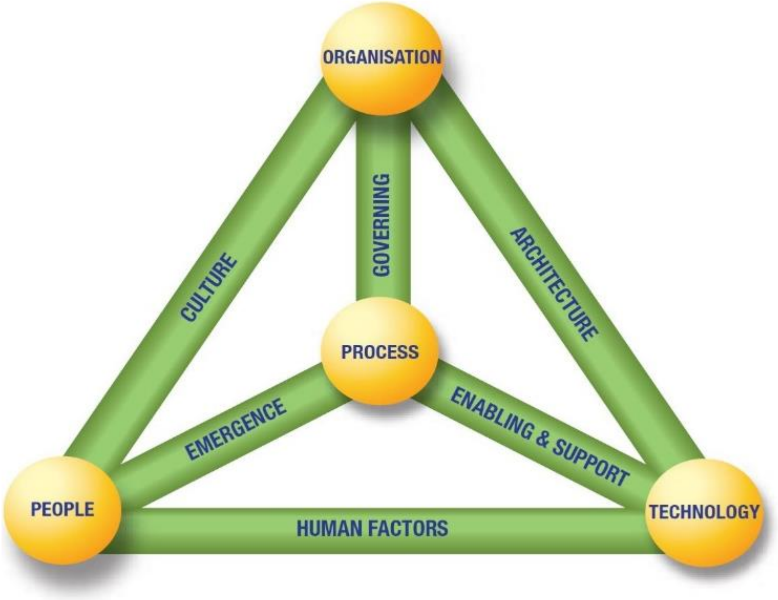


Figure 7: Business Model for Information Security (Kiely & Benzel, 2006), (Roessing & Information Systems Audit and Control Association, 2010)

The systems thinking approach to the organization is achieved through the four elements/nodes in the BMIS model (Figure 10), which was already presented in the introductory chapter, that represent different views of the organization as a whole. The four concepts on the nodes and the interconnections, or "tensions" as Kiely & Benzel (2006) name it, between them, accurately resemble the distinct, but deeply interrelated topics where Information Security risks and corresponding mitigating measures and controls may be expected to impact the organization. Kiely & Benzel (2006, p.4) state the meaning and focus of the four elements as follows:

- The Organization (also sometimes named Organization Design and Strategy) element *"focuses on the need to design organizational structures and strategies that enable the enterprise to compete effectively, create competitive advantages, understand its tolerance to risk and adopt governance policies that elevate security to a first priority, a board level issue, pervasive throughout the enterprise"*.
- The Process element *"means the explicit, formal means by which things get done in an organization"*.
- The Technology element *"is specifically assigned to develop and implement technological approaches to the protection of information systems, approaches that must stay ahead of the competing, threatening technology that would exploit and corrupt those systems if it could"*.

- The People element *"represents the human resources in an enterprise who need to practice not only fundamental security "hygiene," but also, receive added training for securing enterprise data and communications"*.

The interconnections between the main elements are dynamic and represent the competing and conflicting roles between the four elements. For example, the organization needs an official structure, and as such an organizational architecture and implements governance mechanisms to control the structure. As described in the BMIS model literature, governance "sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions" (ISACA, 2009, p. 16). These mechanisms are thus forced upon the organization and its processes, which may hereby be more controllable and measurable but perhaps limited in the effectiveness.

Organization

As shortly described above, the organization perspective focuses on the need for strategy and structure in order to govern the organization and its people, processes and technology in a way that both enables the organization comply to relevant laws and regulations, and derive competitive advantages from its key activities. On the subject of Information Security and privacy, the security risks and the privacy laws and regulations urge the organization to include the development and maintenance of an InfoSec capability in the strategy, and govern the accomplishment of that capability by the people and in the processes and technology. The accomplishment can be reached by focusing on culture, governance of processes, and the architecture of the organization. Regarding the cultural factor an organization can define the values and missions that are communicated to the people in the organization, while regarding processes and technology the organization can define policies that need to be followed for the secure, but also efficient development implementation and execution of processes and supporting systems.

However, before the organization can focus on strategizing on InfoSec the constraints and boundary conditions have to be determined. This includes determining risks in order to focus the strategy, and business objectives that need to be included to define the boundaries on InfoSec from the business perspective such as budget and effectiveness requirements.

The activities from the organization perspective include:

- Setting an Information Security policy that sets a significantly high security level for the organization, and take into account the objectives, requirements and limitations of the business.
- Periodic execution of risks analyses on the processes and technology in the organization.
- Appointment of responsibilities for security and risk management in the organization.
- Setting lines for periodic auditing and evaluating the processes and technology in the organization.

Process

The process element provides a view on information security based on the formal and informal mechanisms that enable the accomplishment of business objectives in the organization. These formal and informal mechanisms are strongly influenced by the governance policies as set from the organization perspective, the habits and culture of the people that execute the processes, and the characteristics of the technology that enable and support the processes. ISACA (2009, p. 15) argues that in the processes, the organization actually manages to "identify, measure, manage and control risk, availability, integrity and confidentiality, and ensure accountability".

The processes in an organization are in operation in order to meet business requirements and objectives. However, while meeting these requirements is the primary goal, the processes should be aligned with policies so that they, the processes, comply with various regulations, including laws regarding privacy and InfoSec but also regarding working conditions. Therefore it is key that policies, from the organization element, are actually implemented and followed in processes. To a large degree, the final responsibility for the alignment with policies lays with the people that execute the processes, but nowadays many policies are also integrated into processes through hard-coded rules and controls in IT applications.

Key activities for InfoSec from the process perspective are:

- Alignment of business requirements and policy
- Alignment of IT with business requirements
- Documentation of processes and communication with people/human resources
- Periodical process audits to determine operational effectiveness of security, but also efficiency and effectiveness with regard to meeting business goals

People

The people element "represents the human resources and the security issues that surround them" (ISACA, 2009, p. 15). The human resources are in the end the actors that implement and execute the policies and processes in an organization, while it is one of the hardest elements in an organization since many human factors, such as values, behaviors and biases, must be taken into account. As can be perceived from Figure 6 in section 4.2 a research by the Ponemon Institute (2013) found that on average 35% of security incidents comes from human errors (not even considering the insider threat), which further increases the urgency for properly managing the people element.

Central in the accomplishment of InfoSec is, according to the BMIS literature, the organizational culture with regard to security. In the BMIS documentation Roessing & Information Systems Audit and Control Association (2010) propagate the formation of an "intentional information security culture" as the key requirement to the successful functioning of information security measures. It is argued that various factors contribute to the incorporation of a security element in the existing organizational culture. ISACA (2009, p. 12) state three specific practices that need to be introduced, 1) security awareness programs, 2) cross-functional (project) teams, and 3) management commitment.

The first practice, security awareness programs, helps to create knowledge about security threats, the necessity of security measures, and the responsibilities of the people in management and on the work floor, while the second measure helps to bridge the gaps between the business, IT, and security. The last practice, management commitment, provides the urgency for the people on the work floor on which the organization to a large degree depends with regard to the actual execution of measures.

Besides the creation of an intentional culture in an organization there are many other factors that influence the Information Security from a people perspective. Firstly, the HR department has to control the stream of new entrants in the organization through proper recruitment, while in addition managing promotion or outflow of current human resources. Furthermore, the roles (functions) and responsibilities of people in the organization and in processes should be clearly defined so that a proper access rights distribution can be achieved.

Factors that influence the successful operation of InfoSec from the people perspective include:

- (Top) Management commitment
- Cross-functional project teams
- HR management policies regarding 1) recruitment, 2) contract management (initiation, promotion, termination), 3) security awareness programs, and 4) function documentation and access rights distribution
- Clear definition of change management procedures
- Task-Technology fit

Technology

The final BMIS element, technology, stands for the IT that to a large degree facilitates the achievement of business objectives set by the organization by enabling the efficient execution of processes. Here IT stands for the total landscape that the organization deploys, which is composed of the applications and their corresponding databases, the supporting operating systems, the network, the underlying hardware infrastructure and the architecture that outlines how all IT is related and connected in the organization.

Although technology is at first a crucial enabler of preventive and detective security measures, such as access management, implementation of (general and specific) IT controls in processes, and active logging and monitoring. However, the technology element is also a source of a broad and dynamic range of risks when people and/or IT are not managed properly; according to research by the Ponemon Institute (2013) "system glitches" make up 29% of security incidents. Vulnerabilities may arise when new features or applications are implemented, the access rights distribution is not properly controlled and audited, operating systems are not timely patched or phased out, old systems or data carriers are not disposed of properly, et cetera. In addition, human factors, such as the resistance to change or accept technology, lacking security knowledge and awareness, or simply human mistakes, cause risks that may impact the confidentiality, integrity and availability of information.

Concluding, from the technology perspective there are numerous factors to enable proper functioning of Information Security:

- Inclusion of procedures and policies regarding management of technology in the security policy
- Alignment of the business and IT (through architecture, people, and application usability)
- Proper identity & access management
- Design and implementation of IT controls in processes
- Monitoring of the IT environment (applications, databases, hardware, network)
- Focus on the awareness and knowledge level of users (in cooperation with HR)
- Budget for technology
- Change management practices regarding implementation of changes

2.3.2. Information Security standards and best-practices

In the section above on the BMIS perspectives we have listed numerous high-level factors that influence the control over InfoSec in the organization. Countless standards and guidelines on Information Security are issued that aim to offer organizations insight in the way in which control over the factors we have mentioned (and more) can be approached. These standards and frameworks are often based on proven solutions and best-practices, or on high-level descriptive theories on how an organization should approach InfoSec in order to develop a mature Information Security capability. Examples of standards issuing organizations are the International Organization for Standardization (ISO), the Information Systems Audit and Control Association (ISACA), The Open

Group, the Information Security Forum (ISF), and the National Institute of Standards and Technology (NIST), but standards and guidelines are also often issued by (semi-)governmental organizations such as the CBP or the European privacy supervisor.

Influential for the Dutch health insurance sector are the ISO/IEC 27000 Information Security standards range and COBIT 5, on which many DNB controls are based. In addition to the ISO/IEC 27000, the CBP offers a more practical guideline that offers a concrete insight in measures that may be taken by an organization to attain the ISO standard and the requirement in the DPA. These standards and guidelines will shortly be discussed here to present the main lines of thought behind these publications.

ISO/IEC 27000

The ISO/IEC 27000, also known as the "ISMS Family of Standards" or ISO 27k, is a range of Information Security management standards that, simply said, provide an oversight of InfoSec requirements, measures and controls that an organization should be able to fulfill to achieve the mitigation of InfoSec risks. The ISO 27k series is generalized, although sector-specific subsets, such as the NEN-7510 for the Dutch health sector, do exist. The ISO 27k range currently consist of numerous general and more detailed standards regarding information security, risk management, cybersecurity, network security, implementation guidance, controls for auditors, etc. the most important of which are ISO/IEC 27000 – overview and vocabulary, ISO/IEC 27001 – Information security management systems requirements, and ISO/IEC 27002 – Code of practice for information security management. The ISO/IEC 27000 standards, however, are quite abstract and high-level, and, in general, do not provide organization with the intended grips to derive at concrete security measures. As such, there are also institutions that offer guidelines that provide organizations with a practical translation of the ISO 27k requirements.

Central in the ISO 27001 "Information Technology Security Techniques" is the suggestion of an Information Security Management System (ISMS) approach to contain and control information security risks in the organization. It states that the organization should take a "*plan-do-check-act cycle*" approach, of which a graphical illustration is given in Figure 8, to the development, implementation and maintenance of InfoSec measures and controls in the organization. (ISO/IEC, 2013)

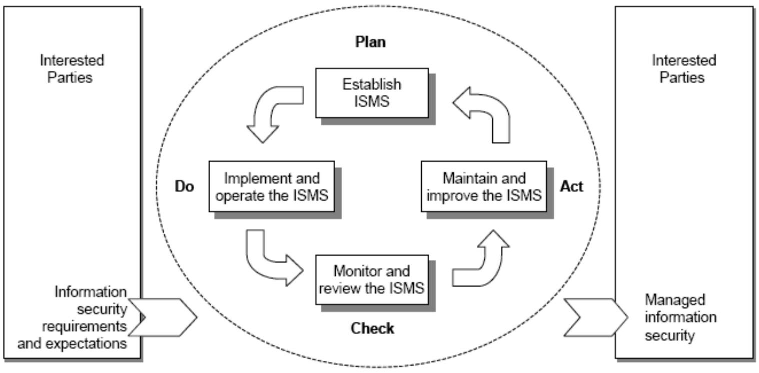

Interested Parties
Information security requirements and expectations
Plan
Establish ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested Parties
Managed information security

Figure 8: Plan-Do-Check-Act Cycle applied to ISMS-processes (ISO/IEC, 2013)

For a more detailed insight in the measures proposed in the ISO 27000 standards range we refer to the ISO 27000, 27001, and 27002 documents of 2005 and 2013.

COBIT 5

COBIT, which is an abbreviation for Control Objectives for Information and Related Technology, is a framework developed by ISACA with the purpose of providing an organization with tools for governing and managing IT and information in processes. The COBIT framework was first released in 1996, and the current version, COBIT 5, dates from 2012. COBIT was developed in order to align IT resources and processes with business objectives, quality standards, monetary controls, and security needs. The idea behind the COBIT framework is that information is needed to support business objectives and requirements. Although the main focus of COBIT is on the governance and control of enterprise IT, the framework also presents aspects to ensure appropriate Information Security in a special professional guide called COBIT 5 for Information Security. (ISACA, 2014)

In the COBIT for Information Security guide, ISACA defines information security as *"something that ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability)",* which is a basic, general, definition that also includes the influential CIA principle that was described earlier in this thesis.

COBIT is based on five key principles which, applied to information security of personal data, state the following:

1. Meeting stakeholder needs – keeping personal data safe for the consumer, and fulfilling the requirements of the relevant supervisory bodies.
2. Covering the enterprise end-to-end – integrating information security in the nature of the company, covering governance, execution, and management.
3. Applying a single integrated framework – aligning enterprise, IT-related and information security related standards and frameworks to provide an overarching framework.
4. Enabling a holistic approach – allowing the organization to form a broad view of Information Security and the impact of measures throughout the organization.
5. Separating governance from management – while governance ensures that all stakeholder needs are balanced and taken into account, management has the responsibility to plan, build, run and monitor measures and controls in alignment with the governance directions.

As can be perceived from COBIT principle 5 and the COBIT (4.1) framework in Figure 9, the first two rings are part of governance, and responsibility of the board, while the more internal rings, the actual execution, are the responsibility of management. Since COBIT aims to provide an integrated framework it is no surprise that we also see the ISO 27k plan-do-check-act cycle, although in a slightly different form, in this framework. The four COBIT "domains", "plan and organize", "acquire and implement", "deliver and support" and "monitor and evaluate", together consist of 34 high-level control objectives and 318 detailed control objectives. These control objectives make COBIT a comprehensive framework for managing risk and control of information and related technology. (Robles, Choi, Cho, Lee, & Kim, 2009)

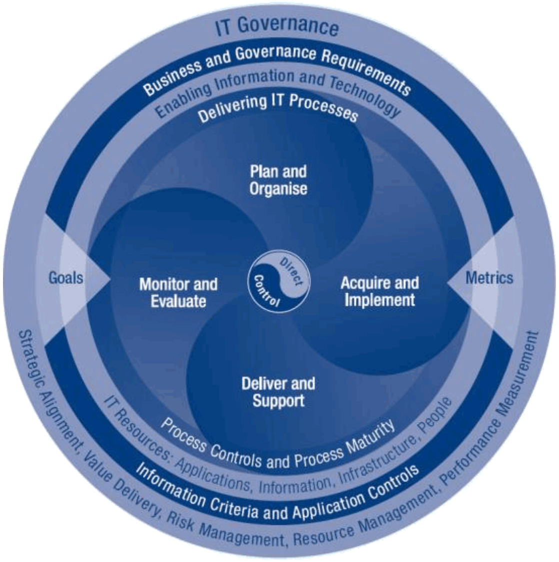

IT Governance
Business and Governance Requirements
Enabling Information and Technology
Delivering IT Processes
Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate
Direct Control
Goals
Metrics
Process Controls and Process Maturity
IT Resources: Applications, Information, Infrastructure, People
Information Criteria and Application Controls
Strategic Alignment, Value Delivery, Risk Management, Resource Management, Performance Measurement

Figure 9: The COBIT 4.1 Framework (ISACA, 2014)

The figure above is derived from COBIT 4.1 but is still applicable, although COBIT 5 is more extensive since it also consults and integrates IT risk frameworks, the BMIS model and the Information Technology Assurance Framework (ITAF). As such, both the general COBIT framework and the COBIT for Information Security framework provide dozens of guidelines, measures and controls for the organization that enable the formation of IT governance, and the design, implementation and operational monitoring, and assurance of processes, and information security measures in processes, in the organization. (ISACA, 2014)

As described, the COBIT framework has been taken into account in this research. However, the framework is too extensive to further discuss here in this thesis. Therefore, we refer to the COBIT documentation on the ISACA website for further information. (ISACA, 2014)

CBP guidelines

In order to give organizations a more practical insight in the requirements that the Dutch DPA imposes on organizations the CBP (2013) has presented a 44 page guideline, which provides a basic interpretation of the law and the measures that are practically required for the security of personal data. The guideline briefly translates the requirements in the DPA into measures that an organization must effectively implement to become compliant. A comparable document will also be periodically issued by the European Data Protection Board when the GDPR becomes active, as stated in Article 66 paragraph 1(b) of the GDPR. (European Parliament, 2013)

The Dutch CBP adds to the ISO 27000 plan-do-check-act cycle the classification of InfoSec measures into the *prevention, detection, and recovery (repression and recovery)* categories as a key activity for InfoSec risk management, and the InfoSec process as a whole. The scheme in Figure 10, translated from the CBP guidelines, gives the threat central elements for risk management related to InfoSec, and for every element states the type of measures that need to be taken in order to minimize risk and impact of a security incident. (College Bescherming Persoonsgegevens, 2013)

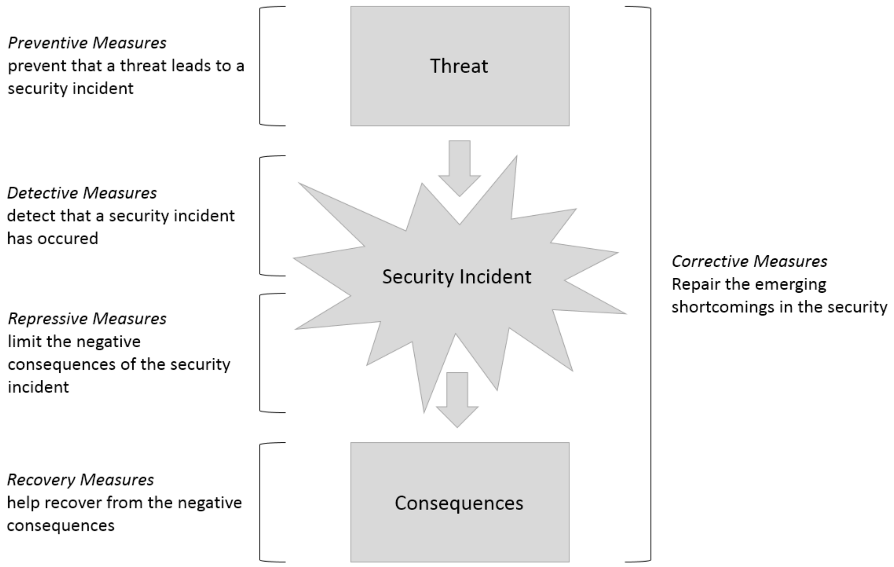

Preventive Measures
prevent that a threat leads to a security incident
Detective Measures
detect that a security incident has occured
Repressive Measures
limit the negative consequences of the security incident
Recovery Measures
help recover from the negative consequences
Threat
Security Incident
Consequences
Corrective Measures
Repair the emerging shortcomings in the security

Figure 10: InfoSec risk analysis elements and corresponding measures (translated from)
(College Bescherming Persoonsgegevens, 2013 p.15)

The Preventive measures are designed and implemented to be able to mitigate the occurrence of security incidents, by containing a threat/risk before it occurs. Many of the measures that should be taken by an organization are preventive in nature, including measures such as:

- A security policy
- Risk analysis & management
- General IT Controls implementation
- Process & IT auditing for vulnerabilities
- Identity & Access Management (logical and physical access), including identification, authentication and authorization
- Network security, including network segmentation and firewalls
- Segregation of duties
- Employee security awareness

As follows logically, detective measures are designed and implemented to detect a security incident at the moment of occurrence or shortly afterwards, so that the likely negative consequences of an incident can, on turn, be contained and limited through responding with Repressive measures. Detective measures include logging & monitoring of hardware, applications, the network environment, access controls, and measures such as virus scanning, etc. Repressive measures depend on the nature of a detected incident, and may include going offline or decoupling a network segment, excluding the threat from the network, removing Trojans/viruses/malware, the appointment of a CERT, et cetera.

After the occurrence of a security incident the organization may need to recover from the negative consequences that result from the incident. Therefore, the organization is likely to take Recovery measures that help to ensure the continuity of the business by taking measures such as setting up a secure environment, recovering data, restarting processes, and informing supervisors, customers, and media.

Throughout the process, but most significantly after a security incident, the organization has to set out corrective measures to repair shortcomings in the security that have led, or may lead to security incidents. Shortcomings may come to light during day-to-day work because of an aware employee, through audits of the organization’s processes or IT environment, or as a result of a security incident that was detected through the detective measures. Corrective measures include (timely) patching of software related vulnerabilities, redesign of measures or whole processes as a result of audits, correction of the access rights distribution, etc. depending on the nature of the risk or vulnerability.

Repressive, recovery, and corrective measures can, in the author’s opinion, all be seen as responsive measures whereby this model can be mapped on the prevention, detection, response models that are more commonly found in literature.

Since the CBP’s guideline is an extensive, but relatively general guideline we will not discuss it further. For a more detailed insight in the measures proposed by the CBP we refer to the guideline document on the website of the CBP (in Dutch). (College Bescherming Persoonsgegevens, 2013)

Comparable guidelines and standards

Besides the more common guidelines and standards such as those mentioned above there are numerous other forums and institutions that present guides to InfoSec and compliance to regulations. As mentioned, The Open Group is an example of an organization that, in contrast to the International Organization for Standardization (ISO), issues an extensive collection of open source standards and guidelines for InfoSec. In one of the interviews we also came across the standards and guidelines of the Information Security Forum (ISF), which is a forum of which an organization can become member. The members of the forum share insights and join resources to collectively research, of finance research into InfoSec and issue best-practices guidelines. Besides COBIT, an alternative reference framework for the alignment of business and IT is ITIL (Information Technology Infrastructure Library), which provides a set of best practices from various public and private sectors.

2.3.3. Factors that influence the realization of Information Security in practice

There are dozens of factors influencing the adoption and realization of an InfoSec function/capability in an organization. Firstly, there has to be urgency for the organization to develop an InfoSec function, since it requires a significant investment of resources while the contribution to productivity is practically zero. Secondly, top management has to propagate a vision and leadership, and develop policies, following the standards and guidelines presented above, that set out the lines for InfoSec.

However, for the practical realization there is another important factor that was also mentioned above, the employees in the organization that have to work according to the prescribed policies. To a large degree the InfoSec measures that people work with on a daily basis are technological in nature and may be innovative for the organization. Therefore we might be able to explain their behavior towards acceptance and realization of InfoSec through the technology acceptance theories and models that exist in the Information Systems research field. These models are based on the Theory of Reasoned Action (Ajzen & Fishbein, 1970) and the Theory of Planned Behavior (Ajzen, 1991), which are models that attempt to explain and predict behavioral intention, behavior, and attitude of people towards changes.

The information systems research field knows three main theories/models that attempt to explain behavior towards changes in the IT environment, namely the Technology Acceptance Model (TAM) (Davis, Bagozzi, & Warshaw, 1989), the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh, Morris, Davis, & Davis, 2003), and Innovation Diffusion Theory (IDT) applied to Information Systems (Karahanna, Straub, & Chervany, 1999; Moore & Benbasat, 1991). Since the TAM theory is most simplified and applicable model, and in addition it has the flexibility to incorporate factors and variables from UTAUT and IDT we will use TAM here to discuss the acceptance of InfoSec measures.

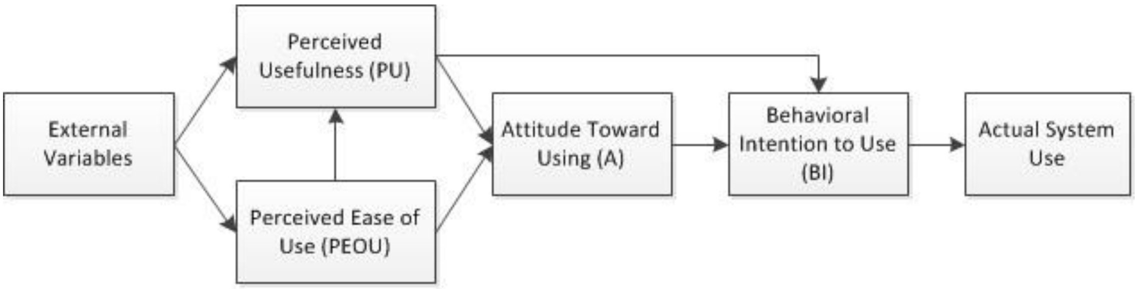

Perceived Usefulness (PU)
External Variables
Attitude Toward Using (A)
Behavioral Intention to Use (BI)
Actual System Use
Perceived Ease of Use (PEOU)

Figure 11: Technology Acceptance Model (Davis et al., 1989)

The original Technology Acceptance Model by Davis et al. (1989) is presented in **Error! Reference ource not found.**. As can be seen the model consists of 5 main factors that are causally linked and influence the actual system use. Two central propositions in TAM are the *perceived usefulness (PU)* and the *perceived ease of use (PEOU)*, which influence a person's *attitude (A) toward using a system* and the resulting *Behavioral Intention (BI)* that leads to the *actual use*. The PU, PEOU, A and BI are characteristics of the individual that works with the technology. Regarding the PU, a person can pose questions such as *"why do I have to use the technology?*", *"does it support me in the execution of my job/function?"*, *"do I support the objectives of the organization by using this technology?"*, and *"what do my colleagues or superiors think of the technology"*, while regarding the PEOU the person can address questions such as *"can I work with this technology?"*, *"how much effort does it cost to work with it?"*, *"am I supported well enough to work with it"*, and *"does it make me do my work more efficient?"*. The answers to these questions lead the person to form an attitude and a behavioral intention towards actually using a system (behavior), and result in the acceptance or rejection of the change. (Davis et al., 1989)

The PU and PEOU are significantly influenced by *external factors*, the factors that come from the person's environment and have a strong influence on his/her perceptions and thus attitudes and behaviors (Davis et al., 1989, p. 987). These factors are not explicitly illustrated in the original TAM, but are further explored in TAM 2 (Venkatesh & Davis, 2000) and TAM 3 (Venkatesh & Bala, 2013), and are often related or equal to factors also named in UTAUT and IDT. TAM 3 explicitly distinguishes the external factors that influence PU and the variables the influence PEOU.

If we map the original TAM and the main perception-influencing external factors, distinguishing between PU and PEOU, on Information Security we derive at the InfoSec technology acceptance model in **Error! Reference source not found.**. As the TAM model is adjusted to Information Security e name this model InfoSec TAM. This TAM model has not been tested since this is out of the scope of this research, but since it is based on common models it should give a good indication of the factors that influence PU and PEOU with regard to InfoSec.

On the operational level we perceive from the InfoSec TAM that the intentional security culture is key to influencing the subjective norm of the people and hereby positively influencing the PU, while training to increase the knowledge level on both security and technology positively influences both PU and PEOU. In addition, the involvement of, and support by management is again a clear factor, which according to this model positively moderates the relation between the external variables and PU.

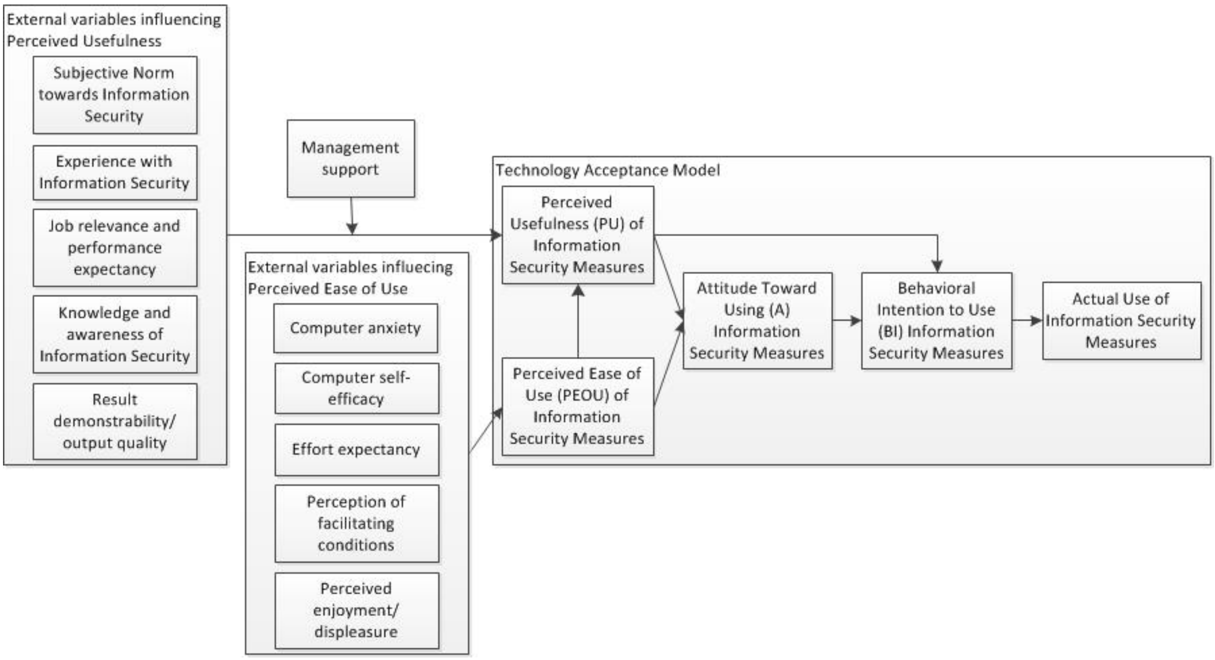

External variables influencing Perceived Usefulness
Subjective Norm towards Information Security
Experience with Information Security
Job relevance and performance expectancy
Knowledge and awareness of Information Security
Result demonstrability/ output quality
Management support
External variables influecing Perceived Ease of Use
Computer anxiety
Computer self-efficacy
Effort expectancy
Perception of facilitating conditions
Perceived enjoyment/ displeasure
Technology Acceptance Model
Perceived Usefulness (PU) of Information Security Measures
Perceived Ease of Use (PEOU) of Information Security Measures
Attitude Toward Using (A) Information Security Measures
Behavioral Intention to Use (BI) Information Security Measures
Actual Use of Information Security Measures

Figure 12: InfoSec TAM: TAM applied to Information Security (Davis et al., 1989), (Venkatesh & Bala, 2013)

In recent literature, the attempt to explain the adoption of InfoSec with TAM has been studied on a small scale. A research by Jones, McCarthy, Halawi, & Mujtaba (2010) finds that TAM is indeed applicable to InfoSec, and concludes that PEOU factors weight heavier than PU factors on the attitude towards use. In addition, a study by Johnson (2005) proposes that the top management decision to invest in Information Security can be explained with TAM. Johnson (2005, p. 116) proposes that external factors that influence top management behavior with regard to InfoSec adoption include:

1. pressures from the external environment;
2. prior Information Security experiences;
3. perceived risks of not securing IT;
4. the current InfoSec budget;
5. security planning practices;
6. confidence in InfoSec, and;
7. security awareness & knowledge level.

3. An Introduction to the Dutch Health Insurance Sector

In order to give insight into the research population, the Dutch health insurers, I will firstly give a short introduction into the privacy regulations that insurers deal with, the health insurance market, and the regulatory bodies that supervise the health insurers.

3.1. The health insurance market

The Dutch health insurance market is heavily regulated since a health insurance is compulsory for all inhabitants of The Netherlands. The insurers have to offer a 'basic insurance' with a coverage that is predefined by the Ministry of Health, Welfare and Sport, and includes the general practitioner, hospital care, and medication. Insurers are not allowed to refuse an application for this basic insurance, or to unilaterally terminate the contract with a client. However, in addition to the basic insurance the insurers are allowed to offer supplementary insurances, such as dental care, for which the insurers may require the client to meet extra conditions.

In 2014 there were around 25 health insurance labels that offered basic and supplementary health insurances. These 25 labels are governed by eight insurance organizations, some of which manage the full administration, financial risk, and product development while others form a group in which all organizations act autonomously. In addition, an insurance company may, to a small degree, have binding authority agreements with insurance agents, in which case the insurance agent takes the administrative responsibility while the company takes the risk in return for a fee. (Nederlandse Zorgautoriteit, 2013)

The Dutch health chain is quite complex and includes several commercial and non-commercial parties that ensure the functioning of the system. The information streams among many of the parties that I have identified in the health care chain are presented in Figure 13. Most of the parties that I have identified have a place in the model, except for the health offices that are deployed by the health insurers and see to the execution of the Exceptional Medical Expenses Act (AWBZ) (Dutch: Algemene Wet Bijzondere Ziektekosten).

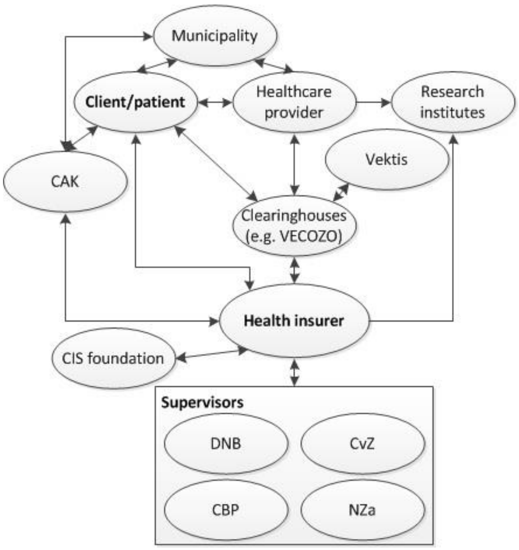


Figure 13: Information streams in the Dutch health chain

Central in the healthcare system in the Netherlands is VECOZO, which is the central clearinghouse through which all declarations flow from the healthcare provider to the health insurers. In certain cases healthcare providers also use their own administration services provider for the administrative settlement, mostly in cases that medical expenses are not always covered such as dentist's bills.

These offices are handle the transactions between the health provider and the insurer, and send bills to the patient in case his/her insurance doesn't cover the treatment. Care providers and insurers are identified through a unique UZOVI-number that uniquely identifies parties in the declaration process. The standard for declarations in this process is managed by Vektis, and prescribes the way care providers and insurers communicate about patients/clients. These standards mostly include standard communication forms that, for example, contain identification information on the patient (including BSN/social security number) and the Diagnosis Treatment Combination (DTC) (Dutch: Diagnosebehandelingscombinatie (DBC)) that the patient/client has received. The standards also include the list of all DBC's that a can possibly occur in practice at the health provider, the DBC's are used to measure the number of treatments of a particular kind and to make a declaration to the health insurer.

3.2. Health insurers

The market, of roughly 16.8 million people, is heavily concentrated considering that the four main organizations together have a market share that exceeds 90%, as follows from market research by the Nederlandse Zorgautoriteit (2013), the Dutch Healthcare Authority. The results of this research are displayed graphically in in Figure 14 and Figure 15. A note that must be made here is that within the larger organizations there may be labels that act as autonomous instances and individually supervised by the DNB, an example is De Friesland within the Achmea group. As can be seen in the figures, the remaining five organizations have market shares ranging between roughly 3.1% and 0.8%. On the basis of this difference in market share I will divide the research population into large and small organization, with a typical market share of >10% for large, and <5% for small organizations. (Nederlandse Zorgautoriteit, 2013)

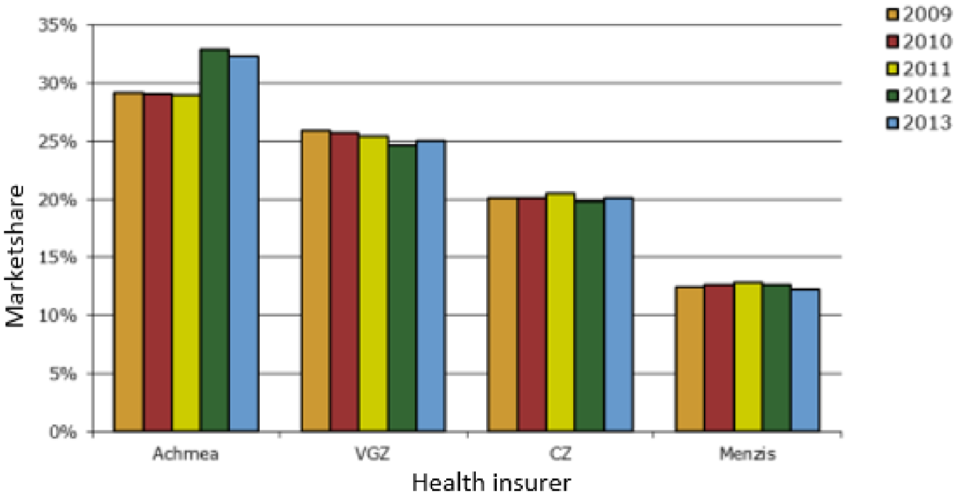


Figure 14: Market shares of health insurers 1 (Nederlandse Zorgautoriteit, 2013)

The Dutch health insurance market has become more concentrated through the years, in 2004 there were 15 insurance organizations that offered health insurances. Many of those organizations sold off their health insurance branches when in 2006 a new health insurance system was introduced. In this way, for example, the health insurance department from Delta-Lloyd and Ohra have become part of CZ.

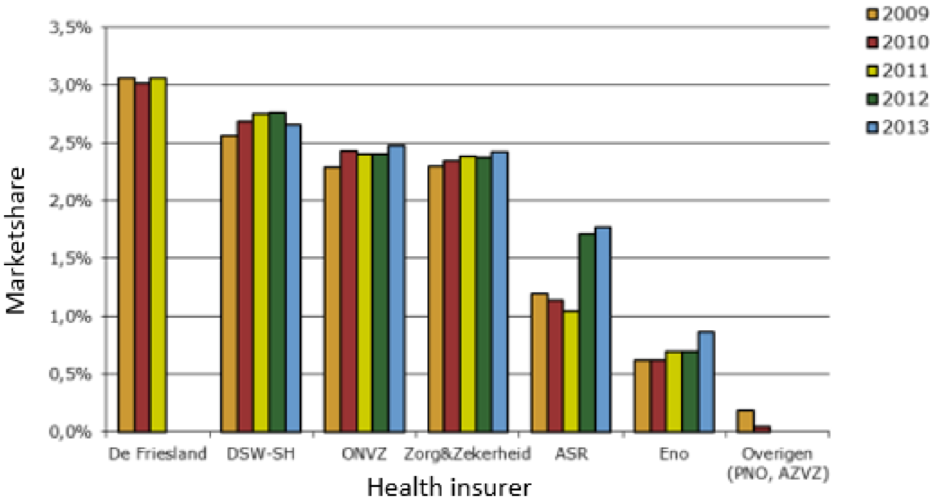


*Figure 15: Market shares of health insurers 2 *De Friesland has merged with Achmea in 2011 (Nederlandse Zorgautoriteit, 2013)*

3.3. Regulators in the health insurance sector

In the Dutch health insurance market there are several regulatory and supervisory authorities that have a stake in the insurers' activities. The Dutch health insurers are supervised on various fronts by De Nederlandsche Bank (DNB, the Dutch central bank) the financial industry supervisor, the healthcare sector supervisor Nederlandse Zorgautoriteit (NZa, the Dutch Healthcare Authority), the supervisor Healthcare Insurance Institute Netherlands (CvZ/ZIN) on the execution of health insurances, and the consumer privacy protection supervisor the College Bescherming Persoonsgegevens (CBP, the authority for the protection of personal data). All of these authorities have differing functions, the DNB primarily focuses on the health of the financial corporation with respect to capital buffers but secondarily also supervises prudential measures for the protection of business continuity (hence also InfoSec), the NZa primarily focuses on the provision of healthcare and the protection of the patient, while the CBP supervises the protection and rightful usage of personal data in all companies in The Netherlands. In addition, these authorities have different degrees of influence on the InfoSec function at insurers. The DNB, for example, cannot enforce their rules on information security with fines, while the CBP has the ability to impose sanctions through the Dutch judicial system on the basis of the Dutch Data Protection Act (DPA).

Despite the fact that InfoSec is not their primary supervisory goal, DNB and NZa both see InfoSec as a key activity for health insurers. Both authorities recurrently investigate the state of InfoSec and present research reports and analytical frameworks for institutions to get insight in the InfoSec function and to highlight vulnerabilities. However, they only have the ability to raise the alarm at institutions that their InfoSec function has vulnerabilities, and as a last resort expose a company to protect consumers when the situation becomes too precarious.

As mentioned, the CBP supervises the care for privacy sensitive data by companies that process personal data, such as health insurers, and cares for the execution of the Dutch DPA that gives legal instruments to govern the protection of personal data. If a data leakage or theft occurs and the company is not able to signal the occurrence to the CBP a fine can be imposed on the company.

4. Relevant privacy laws for health insurers

Regarding privacy regulations, the Dutch health insurance sector is subject to the Dutch Data Protection Act, or in Dutch *"Wet Bescherming Persoonsgegevens"*. The DPA was initiated in the 1990s and accepted by the Dutch Upper House in the year 2000. The DPA is based on the European Data Protection Directive 95/46/EC, which was a response to the emergence of the "Information Society" and had the purpose of protecting citizens for the dangers that come with this new reality in which data is more valuable than ever. In the eyes of the regulator the citizen needed protection from the unethical processing of data, and the inaccurate protection of data by organizations that the citizen places trust in. (Staten-Generaal, 1998)

4.1. The Dutch DPA

The Dutch Data Protection Act is applicable to all processes in which personal data of an identifiable natural person is processed, both automated and manually, and are destined to be recorded in a file (WBP, article 1:1 + article 1:2). Personal data are not explicitly defined in the texts of the law, but in general can include address details, name, date and place of birth, social security number, et cetera.

The DPA differentiates between "general" personal data such as address details, and "special" personal data such as religion, race, political preferences, and health. In article 2:16 of the DPA it is stated that processing of special personal data is prohibited by law, except when the controller satisfies specific conditions as stated in article 2:17-24 of the DPA. Article 2:21:1 concerns exceptions on the processing of health data, and it states that health insurers (2:21:1b), and organizations involved in healthcare, are excluded from the prohibition to process health data. As such, organizations delivering health care related services can carry out their task with the data they need.

In the DPA, various actors are named that are relevant to the processing of data. The most important actors are the data subject, which is the person behind the data, and the responsible organization, which is the organization that carries the main responsibility for the data.

Before an organization is allowed to process personal data, the organization should notify the CBP of this intention. The notification is required by law in chapter 4 article 27, while the specific requirements for the notification are stated in article 28. The notification of a process, or a change in a process, should be made before processing starts. The CBP keeps a record of all processes (of which the CBP is notified) in which personal data is processed.

Although the DPA gives conditions which an organization should fulfill for the rightful processing of personal data, there are no specific security measures suggested or required. In article 13 it is only mentioned that the responsible party:

> *"shall implement appropriate technical and organizational measures to secure personal data against loss or against any form of unlawful processing"* (DPA, article 13 free translation, CBP)

In addition it is stated that these measures:

> *"shall guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected"* (DPA Article 13, free translation from (Council of Europe, n.d.)).

It follows from this article that the level of security should be proportional with the sensitivity and volume of the data that is being processed in the responsible organization. This means that small organizations that deal with sensitive data of possibly thousands of consumers, such as the smaller health insurers, should attain a high information security maturity level.

In case a third party is involved in a process, the principal organization carries the responsibility that the third party deploys sufficient technical and organizational security measures for the data processing. According to DPA Article 14:2 these security measures should be defined in an agreement between the parties.

Compensations & sanctions

In case an organization does not meet the requirements and terms in the DPA, and thus is incompliant with the law, there are three distinct actions through which an organization can be confronted. Firstly, a data subject can take steps on the basis of the DPA. From these steps a number of consequences can result, such as compensation for possible damage to the data subject. Secondly, the public prosecutor can impose a fine on the responsible organization of between €2.250 and €4.500, in case:

- no (proper) indication of the processing of personal data is given;
- no (timely) indication of changes in the processing of data is given;
- no track of abnormal processing that differs from the initial process is available;
- the organization acts in conflict with a ban by the ministry of justice by forwarding data to a land outside the European Union;
- there is no appointed person or instance that acts on behalf of the organization when the organization is not located in the Netherlands or another EU member state, while the organization does process data in the Netherlands with or without automated means.

Thirdly, the CBP can take various actions in case of incompliance. The CBP has the right to use administrative enforcement or impose a financial penalty when one or more terms in the WBP are violated by an organization. Administrative enforcement means the organization gets time to undo the violation before the CBP acquires the right to undo the violation on cost of the organization.

A financial penalty is imposed when the CBP is not able to undo a violation by itself. In this case the CBP can impose a sanction for the enduring duration of the violation. In addition, the CBP can impose a fine of at most €4.500 when the DPA is violated in various other ways.

Since there is no room here to discuss the DPA fully, only the main lines have been discussed here, the full text of the DPA can be found on the website of the Dutch government which includes the law book, Wetten.nl, while an official translation in English can be found on the website of the Council of Europe (Council of Europe, n.d.). In addition, a guideline to the DPA (in Dutch) can be found on (College Bescherming Persoonsgegevens, 2013).

4.2. The European General Data Protection Regulation

A significant change in the privacy regulations is coming in the forthcoming years since the European Data Protection Directive 95/46/EU is being superseded by the European General Data Protection Regulation (GDPR), of which the European Commission released an official proposal on 25 January 2012 as part of a European Privacy Directive. The proposed GDPR is planned to be officially adopted by the European Parliament by the end of 2014 after which a transition period of two years is given to member states to adopt the directive.

The European Parliament presents two main reasons for the reform of the data protection directive. Firstly, the European Commission sees a need for people to become more “in control” of their personal data. Developments such as globalizing data flows, social media, cloud computing, location-based services have significantly increased the risk that people lose track and control of their data. Secondly, the directive is meant to replace the current “patchwork” of national laws. This is intended to both lower barriers for companies to move across the EU, and to strengthen the rights of European citizens. (Aramis Jeanpierre, 2013; European Parliament, 2014)

Since the GDPR is still in the draft phase at the moment of writing it is subject to significant changes that result from the many thousands of amendments that still have to be discussed. However, several expected key points and changes in the GDPR can be stated based on both the 2012 draft, and an unofficial consolidated version of October 2013. This unofficial version results from a vote by the Civil Liberties, Justice and Home Affairs committee and is published by Jan Philipp Albrecht, who is a member of the European Parliament and rapporteur on the EU data protection regulation.

As a first major change, Duthler Associates (2014) notes that the GDPR on norms fundamentally overlaps with current regulations, but in addition provides specified obligations for responsible parties and controllers. This makes the GDPR more concrete than the current directive and the Dutch DPA. Secondly, the law provides numerous articles aimed at giving consumers control over their data, for example through the right to erasure, right to data access and right to correction. Thirdly, article 22 section 8 states that the responsible organization should deploy metrics to assess the effectiveness of security measures. In short, the following list of points and explanations, derived from analyses of the law by Jan Albrecht (2013) and by Duthler & Biesheuvel (2013), give insight in the most influential changes incorporated in the GDPR that are relevant for this research. The unofficial consolidated version of the GDPR of October 2013 is chosen as the main source since this version is the closest to the official version that is expected at the end of 2014.

Future proof definitions

In contrast to the 1995 directive, the GDPR provides an abstract and “future proof” law framework by laying out strong and abstract definitions of terms such as “personal data”, “pseudonymous data”, “data subject”, “processing”, “profiling”, data types (e.g. genetic and biometric data), et cetera. The intention hereof is that the applicability of the law is not influenced by future developments in data processing and IT, with new trending terms such as with the current “Big Data” trend. Several of the important definitions given in the law texts are presented here:

Personal data

The GDPR definition of personal data (version 12-3-2014, article 4 section 2):

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person*

Controller

The GDPR definition of controller (version 12-3-2014, article 4 section 2):

> *'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by Union law or Member State law, the controller or the specific*

> *criteria for his nomination may be designated by Union law or by Member State law;*

Processor

The GDPR definition of processor (version 12-3-2014, article 4 section 2):

> *"processor" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;*

This means that the controller is in the end, from the viewpoint of the law the responsible party for the data processing that occurs in the controller organization or, possibly, at a third party when the controller has outsourced (part of) the process.

Processing

The GDPR definition of processing (version 12-3-2014, article 4 section 2):

> *"processing" means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.*

For a more elaborate list of important definitions we refer to the GDPR law text in the unofficial consolidated version of 22 October 2013 as provided by the member of the European Parliament, and rapporteur on the GDPR, Jan Albrecht. (European Parliament, 2013)

Explicit consent, transparency & other principles

In the new GDPR, transparency and consent are two great pillars for enforcing trust between the data subject and the controller, as the actor mainly responsible for the data. The conditions for consent, as included in article 7, define that the data subject should explicitly give his/her consent for the processing of personal data for specified purposes, and that the controller bears the burden of proof to show that the subject has given his/her consent and has not withdrawn it since.

Regarding transparency there are several provisions that demand the controller to enable the data subject to be fully informed about what personal data is collected, for what purpose, where it is stored, et cetera. In article 5(a) it is stated that the controller shall process personal data "lawfully, fairly and in a transparent manner in relation to the data subject". In the articles 13a and 14 the provision of information to the data subject is described, including the indication of how long the controller is allowed to retain data, and where data it is stored. Through article 15 the data subject is provided with the rights to access and obtain data from the controller regarding the personal data processed about the subject. The controller should then inform the subject on numerous details regarding the processing, such as the purpose of processing, the categories of personal data concerned and the period of data retention, but also the contact details of the supervisory authority and the controller's data protection officer.

Rectification & erasure

In addition to the rights regarding transparency and information of the data subject, the data subject has the right to rectification and the right to erasure of his/her personal data, both of which are included in section 3 of chapter 3.

The right to rectification, article 16, includes that the data subject has the right to obtain rectification of personal data which is inaccurate or incomplete. As described in article 17, the right to erasure includes that the data subject can demand erasure of all personal data stored at, and spread by a controller. When an organization has shared data on data subjects with a third party, for example as part of an outsourcing contract, the organization should also make sure that the third party erases the data concerning the data subject. The claim of a data subject on the right to erasure is, slightly simplified, subject to three conditions:

- the data processing does not comply with EU rules or the data processing otherwise turns out to be illegal;
- the data are no longer necessary for the purposes for which they were collected, or;
- the person objects or withdraws his/her consent for the processing of his/her personal data.

There are, however, situations in which the right to erasure is limited. This may be the case when data is needed for research purposes and the controller has a derogation, the data is needed for purposes of proof (article 17 point 5) or when data retention laws apply or data retention is necessary in the light of a contractual agreement.

Following article 13, the controller shall notify the subject and all recipients of any rectification or erasure that was carried out on the subject’s behalf.

Technological & organizational measures

As described above the GDPR, in contrast to the 1995 directive and the Dutch DPA, prescribes the implementation of concrete technological and organizational data and data processing protection measures in case of an automated processing at the data processor/controller. Most of these regulatory demands for security and responsibility are stated in chapter four of the GDPR.

Article 22 outlines the responsibilities of the data processor/controller, which includes that controllers should implement appropriate policies and measures, and be able to demonstrate that data processing is performed in compliance with the GDPR. The appropriateness of measures depends on factors such as the nature of the data, and the context, scope and purposes of processing.

Data protection “by design” and “by default”, often called “privacy by design”, described in article 23 is one of the key obligations for controllers. Protection by design means that the controller has to implement appropriate protective measures for the protection of data both during process development and process execution, based on state of the art, current knowledge, best practices and the risks present in data processing. Data protection by design is described as follows in article 23(1):

> *“Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data.”*

Data protection by default means that only those data are processed that are minimally necessary for fulfilling the purposes of the processing, and that these data are not collected and retained beyond the minimally necessary time for fulfillment of the purposes of the process. In addition, data are by default not made accessible to an indefinite number of individuals and the data subject should be able to control distribution of his/her data.

In section two of chapter four the main statements regarding data security are presented. First of all this section includes article 30 in which it is stated that the controller or the processor of personal data:

> *"shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, taking into account the results of a data protection impact assessment pursuant to Article 33, having regard to the state of the art and the costs of their implementation"* (article 30(1)).

According to article 30(1a) the policies shall include the implementation of measures and abilities that ensure the confidentiality, integrity and availability (CIA) of the personal data, while the controller should also be able to restore CIA quickly in case of a calamity. An extra note is made on the processing of sensitive personal data, in which case additional security measures are demanded from the controller to be able to take near real-time preventive, corrective and mitigating actions against vulnerabilities or incidents.

In addition to the demands in article 30(1a), the article 30(2) suggests basic measures, which includes that controller and processors should, among other things, be able to restrict access to only authorized personnel, hereby effectively demanding Identity & Access Management. Article 30(3) states that the European Data Protection Board has the task to issue guidelines and best practices, which also includes the determination of the much stated "state of the art" with regard security measures that organizations are expected to implement. In other words, they set the bar by determining what the standard for security is.

Data protection impact assessment and compliance review

Besides the technological and organizational measures demanded in the GDPR, there are also various risk analyses prescribed in section three of chapter four. The requirement of these risk analyses depends on the types of personal data processed, and the risks related to the processing in particular. Depending on the conditions determined in article 32a(3) the controller is obligated to carry out a data protection impact assessment as described in article 33. The data protection impact assessment is an "assessment of the impact of the envisaged processing operations on the rights and freedoms of the data subjects, especially their right to protection of personal data", which, simplified, is an assessment of the impact of the controller's data processing activities.

The prescriptions for the assessment are presented is article 33(3) and includes points such as a description of the processes in which personal data is processed including an assessment of the necessity and proportionality of the processing operations. In addition it includes "a description of the measures envisaged to address the risks and minimize the volume of personal data which is processed" (article 33(3d)), "a list of safeguards, security measures and mechanisms to ensure the protection of personal data, such as pseudonymisation, and to demonstrate compliance with this Regulation […]" (article 33(3e)), and an explanation of the implemented practices regarding the data protection by design and default as required in article 23.

As an addition to the analysis resulting from the terms in article 33, the GDPR also includes, in article 33a, an obligation for the controller to review to what degree the organization achieves compliance with the data protection impact assessment. This assessment should be carried out periodically, at least once every two years or immediately when a significant change in risks in the processing operations arises, for example due to a change in the process itself. Needless to say, the Data

Protection Officer, that will be discussed further on, is involved in all risk analyses and the compliance review in order to control the process and to act as an advisor for the controller.

Notification of a data breach

In the case of a breach of personal data the controller and the processor should, according to article 31 of the GDPR, notify the supervisory authority "without undue delay" which in practice means within 72 hours after initiation of the breach. If the controller or processor reports later an explanation for the delay should be given in the notification. The requirements to which the notification is subject are described in article 31(3) and include the nature of the personal data breach, a description of recommended measures for the mitigation of possible negative effects of the breach, a description of the consequences of the breach and a description of the measures that the controller deploys to address the breach and mitigate its effects. In addition, the controller should appropriately notify the data subjects of which data has been disclosed in the breach.

Controllers should, according to article 31(4), document every personal data breach at the organization very thoroughly, and be able to show adequate documentation to the supervisory authority. The supervisory authority also keeps a public register of the types of breaches that are notified by controllers.

Data Protection Officer

In the current Dutch DPA the appointment of a Data Protection Officer (DPO) is still voluntarily, however in the new GDPR the designation of a DPO will be compulsory, according to article 35, for controllers when they:

- process the data of 5000 or more data subjects in any consecutive 12-month period;
- process data that can be qualified as "special data" as defined in article 9 of the GDPR, or;
- deploy processing operations which involve the systematical monitoring of data.

In this way the appointment of a DPO is not required on the basis of the size of the organization, but on the number of data subjects and the sensitivity of the data.

The DPO has a predetermined position in the organization (article 36), and should, by law, be able to act as an independent authority at the controller organization (article 36(2)). Corresponding to this position the DPO has several specified tasks (article 37) related to the documentation, performance and integrity of the data processing processes, and the information and advisory of the controller and the processor regarding responsibilities and technological and organizational measures and procedures.

Sanctions

According to article 79 of the GDPR a supervisory authority is empowered to impose administrative sanctions on a controller that violates the GDPR. The law states that these sanctions should be determined in each individual case and should be proportionate, efficient and dissuasive. Supervisory authorities should, according to article 79(2a), impose at least one of the following three differing sanctions:

- a warning in writing in cases of first and non-intentional non-compliance;
- regular periodic data protection audits;
- a fine up to 100 000 000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is greater.

The supervisor should take several factors into account when the sanction is determined. These factors are described in article 79(2c) and include the nature, gravity, duration, (un)intentional character of the infringement or incompliance, and the measures deployed by the organization to prevent the infringement or incompliance. If an organization is in the possession of a valid "European Data Protection Seal", as described in article 39 of the GDPR, the fine, may only be imposed is case of intentional or negligent incompliance (article 79(2b)). (Albrecht, 2013), (European Parliament, 2013)

4.3. Impact on health insurers

Since health insurers deal with health data of a large group of people, the strictest requirements regarding care for the protection of privacy are applicable, which is not different from today. However, the documentation of processes, and implementation and operational effectiveness of the required measures is estimated to be much more stringent under the GDPR. An organization is required to be "in control", which means that it should know and document its own processes, risks, and mitigating security and control measures. It is assumed that if an organization does not document its processes it doesn't know them, and as such cannot know the risks and vulnerabilities that may exist. Consequently, an organization cannot mitigate risks that it does not know, whereby a sufficient degree of information security cannot reasonably be assumed.

In order to enforce the achievement of the "in control" status in organizations the GDPR prescribes, as mentioned above, several high-impact measures that health insurers must implement. Firstly, a Privacy by Design/Default approach should be taken to process development, implementation and execution, which is intended to make processes and systems in which personal data is processed inherently secure. This may necessitate organizations to totally revise their approach to process and systems development.

Secondly, the GDPR requires the periodical execution of a clearly documented risk analysis and data protection impact analysis, and based on that a clear mitigation strategy that includes the responsible persons in the organizations that have to see to the actual mitigation.

A third requirement regards the periodical measurement and documentation of the effectiveness and efficiency of security measures and controls deployed by the health insurer, on the basis of which the revision of measures and controls may have to be carried out. Partially this is already a task carried out in IT audits in the context of the financial statement, but these only assess the controls related to systems that have an influence on the general ledger. Therefore, more elaborate process and IT audits on the security controls and measures may have to be carried out by the organization or a specialized and independent party.

Besides, the requirements regarding the "in control" status and the proper documentation as proof of this status, the GDPR requires numerous "standard" security measures to be taken. Examples of these are proper access security, business continuity management, and, more in general, measures that ensure the confidentiality, integrity and availability of the data. For exact details I refer to article 30 of the GDPR.

A relatively minor impact point of the GDPR is that insurers are required to assign a DPO that independently oversees all privacy impacting activities the organization deploys, sees to the honest and ethically just processing of personal data, and supervises the execution of risk analyses and security measures. As was found in a small research on the websites of the Dutch health insurers, at least some of the organization have already appointed DPO's or Chief Privacy Officers, and notified the data subject of their existence on a privacy dedicated part of the website. Some organizations do not provide the name of a DPO, and as such it can be assumed that those organizations have yet to appoint a DPO.

Regarding the GDPR chapter on rights of the data subject the impacts for insurers may be more significant. First of all the data subject has to give a health insurer explicit consent on the processing of his/her data. (S)He has to do this at least at one of the insurers since a health insurance the person is required to have a health insurance. The health insurer then has to be able to proof to the supervisor that a data subject was informed and has given the consent on data processing. Therefore the data subject gives consent through his/her contract with the health insurer, in which case the insurer has to bring into the contract a clearly distinguishable section on consent (article 7(2)).

As opposed to the giving of consent, the data subject also has the right to withdraw consent from the data processor, who is then not allowed to carry out the processing of data related to the data subject anymore. However, this may result in the situation that the insurer cannot insure the subject, whereby the subject violates the law by not being insured. This is the case unless (s)he has already appointed a new insurer, in which case the processing probably stops automatically.

Secondly, the data subject has the right to pursue the correctness of his/her personal data. When the data subject finds that there is incorrect data related to him/her, (s)he can appeal to the right of rectification by which the data processor is forced to correct the data for the data subject. In addition, the data processor should give the data subject the ability to control his/her own data, for example digitally through a web form.

A third right of the subject with, at first sight, a significant impact is the right to erasure, also called the right to be forgotten. In the case a data subject appeals to this right, the data processor should see to the erasure of all personal data relating to the data subject from the processor’s own, and related third parties’ databases. This request can be difficult and time-consuming to fulfill while the risk is high that data remains in (legacy or third party) databases and archives. As such, it can have a high impact on the data processor.

However, this right is subject to numerous conditions. Firstly, according to the article on the right of erasure the data should not be subject to data retention laws, which for health insurers do count. Secondly, the data should not be part of a contract that the health insurer has to fulfill for the data subject. Only when the health insurer doesn’t use the data for processing purposes anymore, and there is no obligation by law to retain the data, then the data subject has the right to ask the insurer to erase his/her personal data. Yet the health insurer is already forced by law to destroy the data subject’s medical files within seven years after contract termination, while files on the data subject’s payment history may be retained for a maximum period of five years. Nevertheless, there is a significant burden on the data processor for keeping registers on where data on specific data subjects is stored, and with which partners it has been shared. (Nederlandse Zorgautoriteit, 2009)

Finally, the increased severity of possible sanctions may have a severe impact in case of incompliance, when the organization is liable for a data breach, i.e. it was in the power of the organization to mitigate the breach, or when the organization has not notified the supervisor of a data breach within the requested time period.

5. Information Security Analysis Framework

On the basis of the literature study several constructs and controls from the standards and guidelines will be used to construct an Information Security analysis framework. This framework will be used to analyze the current state of information security at health insurers. On the basis of the results of this analytical framework we should be able to both assess the current state of compliance with the WBP at Dutch health insurers, and bring up vulnerabilities and points of incompliance where insurers should improve.

The framework follows, as previously discussed, the main lines of the Business Model for Information Security (see Figure 10 in the previous chapter) with the elements Organization, Processes, People, Technology. As can be perceived from Figure 16 the approach to the construction of the analytical framework begins with the high-level requirements from the ISO 27k standards and BMIS. A second step was to review the more practical/operational process configuration guidelines and InfoSec controls that are proposed in COBIT, and to a certain degree in BMIS. The final step was to compose a list of concrete and practical questions and statements on the basis of the higher level standards/guidelines and the CBP guideline, the DNB Information Security Analysis Framework, and common sense. Based on this structure a list of 35 questions was composed. Each question has two or more sub statements that have to be scaled on a five level scale which is based on the CMMI maturity model as applied in the ISO 17799 standard (a predecessor of ISO/IEC 27000). The maturity model is slightly adapted for the specific purpose of this research and is shortly discussed in section 5.1.3.

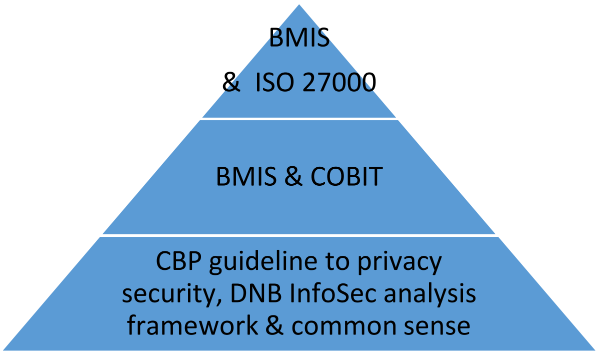

BMIS
& ISO 27000
BMIS & COBIT
CBP guideline to privacy security, DNB InfoSec analysis framework & common sense

Figure 16: Construction approach in analytical framework

Within the four BMIS domains several related subdomains have been added to be able to further differentiate among policies and measures that exist in the framework. These subdomains are only intended to guide the filler through the framework, and do not have a significant role in the framework. As such they will not be described here in detail.

The construction of the framework is discussed in the following section, while the way in which the results from the framework are processed and presented to the user is presented thereafter.

5.1. Framework Constructs

We start this section by shortly describing the general, identifying, questions posed at the start of the framework. These questions are intended to give an insight in the size and activities of the (IT) organization. In the second section we will move on to the presentation of the 35 questions of the BMIS level. After that, the way in which the maturity levels are defined in the framework will be discussed. Finally, this section is completed with a categorization of the questions into 7 distinct groups.

5.1.1. General questions

After the introduction to the framework and the company/user identification we start with a series of general questions that give insight in the nature of the organization, the way in which it approaches and deals with 1) Information Security practices, 2) relevant privacy regulations, and 3) Information Security issues and impacts. These questions mostly take the form of polar (yes/no), or scaled (low/medium/high) questions. In addition, several questions are asked on organizational facts such as the IT (security) budget, number of (IT related) employees, and number of (IT related) security incidents.

The reason behind the incorporation of these questions in the framework is twofold. At first the organization that uses the framework can use the questions to assess the position of the organization with regard to size, security incidents, information security practices, and view of regulations. In addition, it can use these questions to categorize organizations in case of InfoSec benchmarking. Secondly, we aim to collect research data through the framework, and the answers to these general questions can help categorize organizations based on attributes in the population. Besides, it provides additional insights in, for example, the way in which the organizations see the impact of security incidents and privacy regulations.

For an oversight of all general questions we refer to the Excel file of the analytical framework.

5.1.2. Questions per BMIS element

As has been discussed we have used the BMIS model as a high-level outline for the analytical framework. Therefore, the framework consist of four distinct sections with differing questions that are relevant to the specific organizational domain/element.

In addition to the BMIS elements, several "sub domains" have been included in the framework, which are used solely to guide the user of the framework. For the categorization of the results of the framework we will use categories that crosses the boundaries of the specific domains. As such, the sub domains are not relevant to the results.

The main questions posed in the analytical framework are given in Table 2, Table 3, Table 4, and Table 5. The further elaborations on sub statements is not given for the sake of clarity and the space it would take here.

Organization

Table 2: Analytical framework questions on the Organization domain

Strategy & Governance	
1	Does your organization have an IT strategy document?
2	Does your organization have a policy/governance document on InfoSec?
3	Does your organization assign and document appropriate responsibilities for InfoSec in the organization?
4	Does your organization have clearly documented and adequate policies on business continuity management?
5	Does your organization have clearly documented and adequate policies on the management of data leaks and security incidents?
Risk & impact analysis	
6	Does your organization carry out thorough risk management?
7	Does your organization carry out a Privacy Impact Analysis (PIA), a risk analysis specifically related to privacy risks and for impact on the client?
8	Does your organization regularly revise the risk analysis and PIA to include new risks or mitigations?
9	Does your organization determine the priority of InfoSec (in the board/organization) on the basis of the risk analysis and PIA?

Third-party management	
10	Does your organization have strict selection procedures for the assignment of third-parties?
11	Does your organization carry out thorough risk analyses at, and regarding, third-party processors/suppliers?
12	Does your organization set and contractually define security requirements in consultation with third-party suppliers?
Check-ups & evaluation	
13	Does your organization periodically assess/audit the third-party for compliance with security requirements and agreements?
14	Does your organization periodically review and evaluate the adequacy of contracts with third-party suppliers?
Management of person bound data	
15	Does the organization have measures in place to govern purposeful data disclosure to a trusted third-party?

People

Table 3: Analytical framework questions on the People domain

HR Management	
16	Does your organization deploy strict personnel recruitment, promotion and termination procedures?
17	Does your organization check and evaluate security processes and policy knowledge throughout the organization?
Security awareness + Knowledge management	
18	Does your organization create and propagate appropriate security awareness throughout organization?
19	Does your organization create, maintain, and test knowledge of governance documents/ policies throughout the organization?
20	Does your organization deploy thorough handling procedures on physical information assets (e.g. paper, usb-sticks)?

Process

Table 4: Analytical framework questions on the Process domain

General process measures	
21	Does your organization pursue the standardization of change management procedures?
22	Does your organization deploy and maintain segregation of duties?
23	Does your organization actively pursue knowledge transfer regarding processes and operations?
24	Does your organization deploy data management procedures?
Third parties in processes	
25	Does your organization periodically evaluate the dependency or power on third-party suppliers?

Technology

Table 5: Analytical framework questions on the Technology domain

Access control	
26	Does your organization deploy sufficient physical security of premises and data assets?
27	Does your organization deploy a satisficing identity and access management (IAM) system?
Network Security	
28	Does your organization deploy satisficing network security procedures?
IT Management	
29	Does your organization deploy thorough IT lifecycle management?
30	Does your organization actively manage (technical) vulnerabilities in IT and processes?

Auditing	
31	Does your organization check and evaluate security processes to assess the current state of compliance?
32	Does your organization regularly perform audits on the security requirements in IT applications?
33	Does your organization use encryption and/or hashing on data that is classified as highly confidential or personal data?
34	Does your organization use technical measures to maintain and safeguard the integrity of data?
IT Architecture	
35	Does your organization actively pursue a manageable IT architecture?

5.1.3. Maturity model for InfoSec assessment

Since the analytical framework is intended to give insight in the state of the Information Security capability of an organization we need an appropriate maturity model. Maturity models can be used both to assess an as-is situation and to highlight the to-do actions for the development of a specific process or capability in the organization. Throughout the years many different maturity models have been developed for various organizational capabilities and processes ranging from quality management to software development. Obviously, models have also been developed for Information Security. However, the maturity models we found in scientific literature that were aimed specifically at Information Security were not considered fit for the purposes of this research. We found that there was a too narrow focus and we judged that the models would not fit well with COBIT and ISO 27000 models that are used frequently among the research population. (Mettler & Rohner, 2009)

According to Mettler & Rohner (2009, p. 5) we can take a standard maturity model and configure it to the specific needs of an organization by *integrating situativity considerations* into the model. Therefore, we take the Capability Maturity Model Integration (CMMI) as a basis and adapt it to the characteristics of the Information Security capability. Although, the CMMI model is mainly focused on software development processes, it consists of many general concepts which make it applicable or easily adaptable to various sorts of process management, specifically concerning IT.

As an attempt to determine the maturity of an Information Security capability Carbonel (2008) has merged the CMMI and ISO/IEC 17799:2005, the predecessor of the ISO/IEC 27001. The result is, in essence, the model presented in Table 6. This model is slightly adapted from the initial model presented by Carbonel (2008) to suit application in this research. Firstly, the level meanings based on ISO17799:2005 are slightly expanded, and secondly the “non-existent” level is erased since it does not exist in the CMMI model and would not be specifically applicable in this analytical framework since all insurers are expected to at least initially execute the measures in the framework. (Carbonel, 2008) (CMMI Product Team, 2010)

Table 6: Application of CMMI to ISO 17799:2005, adapted for measurement of Information Security maturity. Adapted from (Carbonel, 2008)

CMMI level	Level meaning (based on ISO 17799:2005, chapter 5)	DNB 2014 Maturity criteria (De Nederlandsche Bank, 2014b, p. 3)
-	-	**Non-existent** - No documentation. There is no awareness or attention for certain control.
1: Initial – Process is unpredictable, poorly controlled and reactive.	The security policy/measure is not formalized	**Initial/ad hoc** - Control is (partly) defined, but performed in an inconsistent way. The way of execution is depending on individuals.
2: Managed – Process is characterized by	The documentation or measure exists, and has been	**Repeatable but intuitive** - Control is in place and executed in a structured and consistent, but informal way.

projects and is often reactive.	validated and disseminated, but it is incomplete or does not fit in the context of the organization.	Criteria: The control execution is based on an informal, unwritten though standard practice.
3: Defined – Process is characterized by the organization and is proactive.	The documentation or measures exists, is complete, has been validated and disseminated, and fits the context of the organization.	**Defined** - Control is documented, executed in a structured and formalized way. Execution of control can be proved. Criteria: * Formal control is available for any critical process. * Critical processes and controls are identified based on risk assessments. * There is evidence of implementation of the control * Formal "test of design effectiveness" constitutes evidence for level 3. * Formal "test of operating effectiveness" constitutes evidence for level 3. *The test of operating effectiveness should be done over an appropriate period which fits the risk profile.
4: Quantitatively managed – Process is measured and controlled.	Controls are set up to assess the application of the validated documentation/measure	**Managed and measurable** - The effectiveness of the control is periodically assessed and improved when necessary. This assessment is documented. Criteria for level 3 plus the following: * The periodic evaluation of the control is documented, including any identified action for improvement. *The frequency of the periodic evaluation should be based on the risk profile. * The frequency of this assessment should be at least annually.
5: Optimized – Focus is on continuous process improvement.	A regular reviewed process allows assessing the application of the previously validated documentation/measure and enables the organization to regularly update it.	**Optimized** - An enterprise wide risk and control program provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements. Distinguishing criteria are: * Continuous improvement. * Comparing control performance with market data of other enterprises. * Advanced IT-support as workflow processing and integration.

The official CMMI model consists of two types of maturity scales, notably 1) continuous, which consists of four maturity levels, and 2) staged which consists of 5 maturity levels. The scale proposed in this framework is based on the staged model, which means that the maturity is determined on the basis of a set of security controls for every maturity level. If in practice one of the specific controls that are required for the maturity level is missing, the organization does not attain that maturity level. However, since there are numerous broader controls in the analytical framework presented in this thesis, the application of the pure staged model would become very unclear when used for the analytical framework as presented in this research. For example, the maturity level resulting from the framework might hinge on the maturity level assigned to one of the 160 statements. Therefore we use a continuous model with the five level scale of the staged model.

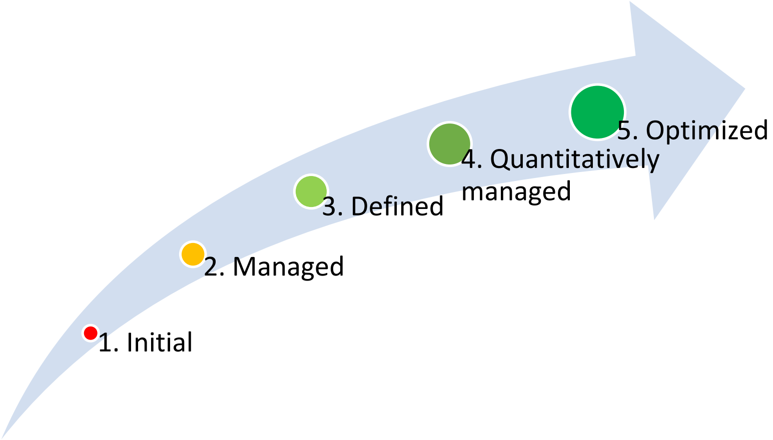


Figure 17: Illustration of the CMMI model, based on (CMMI Product Team, 2010, p. 23)

The CMMI model consists, as mentioned in Table 6 and displayed in Figure 17, of 5 maturity levels, notably: 1) initial, 2) managed, 3) defined, 4) quantitatively managed, and 5) optimized.

5.1.4. Categorization of questions

In order to be able to present a clear oversight of the results of the analysis carried out through the framework we have to categorize the questions at another level than the BMIS elements that are used as the main structure of the framework. An overarching set of 5-10 high-level Information Security requirements or focus areas is needed to properly categorize the answers to the questions as presented in section 5.1.2. The ISO/IEC 27001 standard provides such a categorization in the form of 14 control objective domains (in the 2013 publication), which are listed in Annex A of the ISO/IEC 27001 standard and are numbered A. 5 to A. 18. (ISO/IEC, 2013)

The following control objective domains are included in ISO/IEC 27001:2013 (with indication nr.):

- A. 5: Information security policies
- A. 6: Organization of information security
- A. 7: Human resource security
- A. 8: Asset management
- A. 9: Access control
- A. 10: Cryptography
- A. 11: Physical and environmental security
- A. 12: Operations security
- A. 13: Communications security
- A. 14: System acquisition, development and maintenance
- A. 15: Supplier relationships
- A. 16: Information security incident management
- A. 17: Information security aspects of business continuity management

- A. 18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws

Although this list provides a very complete oversight of control domains, the list is over complete for the purposes of this analytical framework. Therefore, we will group several of these domains together and leave other, irrelevant, domains out. This leaves us with the following seven categorization domains:

- Information security policies & Organization of information security
- Human resource security & Identity & Access Management/Access control
- Asset management & operational security
- System acquisition, development and maintenance
- Supplier relationships
- Business Continuity Management & Information security incident management
- Compliance

The categorization of the questions from section 5.1.2 into the seven categories is based on highest relevance, and can be found in Table 7. Some questions have been assigned more than one time because of their relevance to other categories.

Table 7: Categorization of questions into nine categories

Category	*Corresponding question(s) (see section 5.1.2) from BMIS domains*
Information security policies & Organization of information security	Organization: 1, 2, 3, 9 People: 19 Process: 21 Technology: 29, 35
Human resource security & Identity & Access Management/Access control	Organization: People: 16, 17, 18 Process: 22 Technology: 26, 27, 33
Asset management & operational security	Organization: 3, 9 People: 17, 20 Process: 22, 23, 24 Technology: 28, 29
System acquisition, development and maintenance	Organization: 2 People: - Process: 24 Technology: 29, 30, 31, 33, 34, 35
Supplier relationships	Organization: 10, 11, 12, 13, 14, 15 People: Process: 25 Technology:
Business Continuity Management & Information security incident management	Organization: 4, 5, 10, 12, 15 People: - Process: - Technology: 28, 30, 31
Compliance	Organization: 2, 4, 5, 6, 7, 8, 11, 13 People: - Process: 22 Technology: 26, 32

5.2. Processing of results

The results from the analytical framework can be analyzed and interpreted in various ways. Firstly, the BMIS can be followed and the maturity per element can be estimated. However, this may give a view that has too little detail to point at concrete vulnerabilities or points for improvement. A second way is to group the 161 statements into eight categories, on the basis of which a spider-diagram can be constructed as discussed in the previous section.

These categories broadly represent the Information Security control objective domains from ISO/IEC 27001 fields and can be reviewed by looking back at the answers given on the respective questions that belong in a certain category. An example of a resulting model (randomly generated) is displayed in Figure 18.

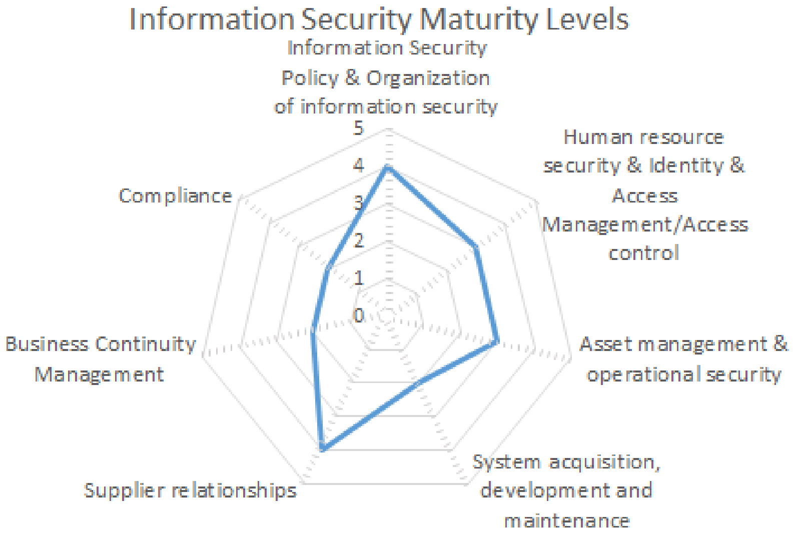


Figure 18: Randomly generated example of an analytical framework result processed in a categorized spider-model.

6. Data collection & verification of the analytical framework

In this chapter we will set out the information regarding both problems and solutions regarding information security problems at health insurers derived from the interviews at three health insurers in the Dutch FSI.

6.1. Methodology

As a recapitulation we shortly discuss the methodology with which this research has been approached. As a first step to the data collection we have created an oversight of the health insurance market in the Netherlands. This oversight is presented in chapter 2, and includes an introduction to the health insurance market and an oversight of relevant laws with the corresponding supervisory bodies. Following the creation of this oversight we have in chapter 4 further investigated current and future privacy regulations to which health insurers are subject. After this investigation we have discussed Information Security vulnerabilities, practices and current literature in chapter 2, on the basis of which an analytical framework for InfoSec was constructed in chapter 5.

Interviews

With the knowledge of the market, regulations and information security several interviews have been conducted with CIO's and Security Officers at health insurers for the purpose of:

- getting insight in the information security practices and the state of compliance at health insurers;
- getting insight in the impact of the WBP, and;
- verifying the Information Security analysis framework.

In order to be able to approach the research population, and especially the CIO's and Information Security managers, various channels have been used among which are 1) the thesis supervisors at the University of Twente and ConQuaestor, 2) LinkedIn, and 3) the Dutch CIO Platform. In this way we have been able to contact all 9 organizations that offer health insurances in The Netherlands. In order to draw their attention for this research we have sent to these organizations an e-mail with attached to it a one-pager on this research and outlined the possible benefits resulting from participation.

Only three health insurers responded positively to this request. We have interviewed one CIO (Director IT & IM, partially fulfills CIO role together with a colleague), three Information Security Managers, and one Data Governance Manager. The three organizations at which interviews were conducted together have a market share of >60%.

In addition, we have received three negative reactions from organizations that did not want to participate in this research. There were two reasons given for the negative responses. The first reason given was that the organization had a policy that a delicate subject as InfoSec is not discussed with outsiders, while a second reason was that organizations thought that the emergence of a new framework besides the DNB Information Security framework would cause confusion in the market.

The basic scripts used for the interviews can be found in Appendix C – Structured interviews, at the end of this report. The interviews were all structured and designed to have an approximate duration of one hour.

For the purpose of minimizing biases in the answers given in the interviews, several statements regarding anonymity have been set. The idea behind this is that with these statements agreed upon, the interviewees can speak more freely about InfoSec practices and their state of compliance. The following statements on anonymity have been proposed to the interviewees:

- The interviewee will receive a copy of the concept thesis research document for review before publishing at the university;
- The interviewer will not use the interview for commercial purposes;
- The researcher/interviewer can request at the university to not have the thesis openly published, or else to apply censoring to leave sensitive data out of the report;
- The interviewee will receive the final thesis and analytical framework when the thesis is finished;
- The researcher/interviewer will sign a non-disclosure agreement if deemed necessary by the organization.

As an additional measure to arrive at more reliable results from the interview, we have chosen not to make recordings of the interviews. On the one hand this benefits the research because of the increased chance that more honest answers to questions are given, but on the other hand the interviewer has to deal with the risk of not remembering important quotes.

The interviews contain four to five sections depending on the question if the insurance organization has more than one label under which health insurances are offered. The first section is targeted at categorizing the organization, which gives data that will only be used when the research group is sufficiently large so that no individual organization can be identified by its size. The second section is targeted at the larger organizations with more than one label. The main purpose here is to determine how InfoSec is managed in the main organization, and to find out to what degree processes and policies among labels are separated.

In the third section, the main section of the interviews, we question the organization firstly on the incidents they deal with in which the CIA principles of data are possibly violated, secondly on the impact and knowledge of the new privacy regulations in the organization, and thirdly on the InfoSec policies and measures that the organization applies to protect the personal data of their clients.

Directly afterwards we have summarized the interviews in as much detail as possible, and sent the summaries to the interviewees for control purposes. These interview summaries have then been reviewed, of which the findings are summarized and analyzed in the interview review in section 6.2.

Framework verification

Since the analytical framework could not be directly tested in the interviews because of time limitations we have, directly after the interviews, asked the interviewees if they wanted to fill-in the framework and return it. The purpose of this data collection step was to collect quantitative data on Information Security besides the qualitative data from the interviews, and analyze the maturity of organizations in the statistical analysis software suite SPSS.

However, most organizations declined the request to fill-in the framework, and only one of the targeted organizations agreed to return a filled framework to me. Statistical analysis of the resulting data is, as such, not possible. Nevertheless, this one result does provide proof that the analytical framework is to a large degree correct and provides an insight in the state of Information Security.

6.2. Interview Review

In the following paragraph we will provide a summary and analysis/review of the interviews that were conducted with five managers at three different health insurance organizations. The review is arranged in sections on different aspects that influence, or are influenced by, InfoSec in the organization. This arrangement corresponds to the structure maintained in the interviews; discussing the organization as a whole, the security incidents and the response to those, the influences of the WBP/GDPR and the compliance to those laws, Information Security and the activities regarding Security Awareness, and finally Data governance. At the end of each section a short recapitulation on the key insights is given.

Organization

In the Dutch health insurance sector there are two types of organizations that we can distinguish, there are, as presented in chapter two, four larger organizations with market shares of >10%, and several small insurers with market shares of <5%. In larger organizations with more than one label, the labels are often centrally managed, but internally divided in separate divisions with corresponding IAM rights and Chinese Walling depending on internal agreements. In the organizations with central management of information security the Governance of IT security measures are often directed to the labels. Sometimes these labels have a high degree of autonomy in the execution of non-technical measures, such as Security Awareness. However, these labels are then individually responsible for the verification and justification of their state of compliance with governance and regulations. Generally this is done through an internal control framework, including the 54 COBIT controls on the basis of which the DNB measures compliance and maturity. The control framework is often aggregated from various individual parts or labels and verified by the central organization, which on its turn reports to the DNB.

Since at the autonomous health insurers InfoSec is managed for that organization only, there is more freedom in the choice of both governance and technological approach to information security. However, according to the law the state of compliance should be comparable to the larger organizations with comparably heavyweight measures for InfoSec. As autonomous organizations are individually subject to DNB supervision, the autonomous organizations/labels are obliged to report to the DNB on the basis of the 54 COBIT controls.

When it comes to Information security and security reporting standards and methodologies, the use of COBIT by the DNB for the supervision on processes seems effective at the insurers. However, in many cases it requires rebuilding or revision of processes to implement a COBIT based control framework to be able to meet requirements, and report to the DNB efficiently. This revision is costly, requires substantial competences, and is resource-intensive, which caused problems at both the smaller and the larger organizations. Besides, in the interviews it was often noted that standards such as the ISO/IEC 27000 are too general and vague to be practically applicable. In addition, the general guidelines in the privacy and information security regulations leave large parts of the structure, construction, and execution of InfoSec to the organization itself. From the interviews it is perceived that this generality causes many organizations to be clueless with regard to the degree of security that is required from them, and the measures that should be implemented.

Key insights:

- In organization with more than one label, processes for different labels are, and should be, separated through IAM and Chinese Walls. Governance is completely or to a large degree equal for all labels.
- Smaller organizations need to comply with the same InfoSec requirements which weighs heavy on their resources.
- Implementation of 54 COBIT controls often requires revision of process(es) in the organization.

- ISO 27000 provides a too high-level insight in InfoSec and is therefore not readily implementable. This forces organizations to go to more practical best-practices guidelines.

Incidents

Considering incidents in which the WBP was violated, all organizations claim that there have not been (serious) incidents, except for one incident that was widely reported in Dutch media. This incident concerned an employee at one of the insurers' IT departments that had left client data on his own, not properly secured, home FTP-server which he used for testing purposes. This situation stayed unnoticed for two years until it was discovered in late 2013. It is not known if the data on the server was actually approached by "hackers" in the time-period that it was on the vulnerable server. (Infosecurity Magazine, 2014)

Except for this one situation there have, at this point in time, not been other known WBP related incidents at Dutch health insurers. However, the insurers indicated that minor internal incidents and vulnerabilities caused by human errors and lack of security awareness occur now and then. For example, it was mentioned several times that official policies regarding data disclosure to people within the company are sometimes not properly followed and a signature from a superior is missing on an official document while data is already transferred or disclosed. Another example is that ordinary USB-sticks are used for classified data, while encrypted sticks are prescribed and available for that purpose. Besides, a security vulnerability that often occurs is the theft of company laptops from cars or in the train, a mitigating measure for this problem is that laptop-drives are encrypted and laptops are locked with passwords.

In several interviews it was noted that the occurrence of security incidents resulting from social engineering may actually exist, but stay unnoticed as a result of the nature of social engineering. In one of the interviews it was argued that it regularly occurs that a call-center employee notifies management of a "strange" or irregular conversation that may be an attempt of social engineering. It remains unclear, however, how many actual (successful) attempts take place since it is unknown how many social engineering attempts stay unnoticed.

Key insights:

- Only one major incident at an insurer is currently known, besides there are regularly vulnerabilities resulting from human errors or lack of awareness.
- Preventive measures for data disclosure are implemented but sometimes not followed out of convenience or lack of awareness.
- It is not known how many attempts of social engineering happen at insurers, and it unknown how many attempts are actually successful.
- Preventive measures to address data disclosure through social engineering are taken.

WBP/GDPR

With respect to both the Dutch and the European Data Protection Acts the knowledge of the regulations, and the priority for compliance is very high at all organizations. Correspondingly, the state of compliance is not that differentiated among organizations. Some organizations are occupied with the professionalization of security measures and policies, such as access rights management and data classification, and all struggle with the *"right to be forgotten"* and the *"right of control over own data"*.

The general opinion among the insurers is that the regulator is right when it comes to the necessity for the protection of the privacy of the customer, and the provision of more control over one's own data. But on the other hand, the insurers state that the regulator does not properly take practice into account when regulations and measures are proposed and imposed on organizations. The documentation, measurement, and justification requirements in the GDPR weigh so heavy that the sentiment among insurers is that they become more supervisors than operators of their own processes. Some stated that the GDPR in some aspects misses its main targets, the social media platforms and marketers of personal data for advertising purposes, while it harms organizations that deal personal data for responsible and justifiable purposes.

In the case of the "right to be forgotten" there is a conflict with data retention regulations that state that healthcare declarations should be kept for at least 7 years in case of declarations from within the Netherlands and 10 years in case of international declarations, not to mention the requirement to keep records on data that is shared with a third-party for 20 years.

When it comes to the control over own data the main thought is that a statement from politics is required. The main problem here is the age at which one becomes responsible for own data, and who is responsible before that age or when one cannot care for himself/herself. Should, for example, a father be allowed to see that his daughter uses anti-conception medication? In some cultures there is a taboo on these sorts of domestic discussions.

Besides the incompatibility of the privacy regulations with other regulations, the health insurers often have to deal with internal problems that prohibit them from properly implementing and executing security measures and policies. Several of those problems will be discussed in the next section on compliance.

Key insights:

- At the insurers we have assessed the current state of compliance appeared to be sufficient.
- All insurers agree on the fact that privacy protection is a key objective for an organization that processes large amounts of very sensitive personal data, and that strong laws and supervision are necessary to enforce this objective.
- The general opinion among insurers is that the requirements in the GDPR are anticipated to weigh disproportionately heavy on institutions, such as health insurers, that know they have to deal responsibly with personal data.
- All insurers were actively engaged in developing measures in anticipation of compliance with the GDPR, but on some points have a difficulty in finding practical solutions to regulatory requirements.

Compliance

In general, all health insurers where interviews were conducted seem to be working on their InfoSec measures and compliance. Besides viewing compliance as an obligation to the regulator they all see it as their duty with respect to the customer that trusts them to safeguard their health data. All insurers indicated that they meet the DNB requirement to be at maturity level 3, and are working on measures to increase maturity to level 4. They also indicate that they do not necessarily do this to "please" the DNB, but also out of their own awareness of the necessity for a mature InfoSec capability. Many insurers indicated the start of significant improvement and professionalization programs around 2010, the year that the DNB InfoSec program started, out of a feel for the necessity of InfoSec.

However, a struggle to comply is seen at both the larger, centrally organized, and the smaller, autonomous, organizations. While the smaller organization in some cases seem to lack resources and power to get InfoSec on track, the larger organization in some respects seem to lack oversight and the ability to comply due to the complexity of their IT landscape's and the presence of legacy systems. Legacy systems carry the problem of incompatibility, these systems are often not adapted to new standards since the cost of maintenance and adaptation are enormous while they are nominated to be phased out.

All organizations indicated that the human factor is key for attaining compliance. Although InfoSec can to a large degree be achieved through technological measures (e.g. network and access security), the human side in the implementation and maintenance of InfoSec measures is harder to achieve, as indicated by the interviewees. Despite the fact that employees are often very aware of the sensitivity of data, the awareness of the necessity for security measures and policies is frequently lacking. Often this comes from the fact that they expect a little trust from their employer regarding their ability to keep data safe. This also follows from the fact that, as stated above, internal data disclosures are sometimes completed without going through the required steps according to the official policies. Despite the fact that the data arrives at the right place, the transfer process should be in accordance with the policies to keep control over data, according to the insurers. To the employee the implementation of restricting policies and measures often seems to be a 'vote of no confidence', an example hereof can be derived from a quote by one of the interviewees:

> *"People do not see the threats in the use of [ordinary] USB-drives for the purpose of storing sensitive data. They have the confidence that they won't lose it and they want their employer to trust them that they won't."*

In addition to the factor of trust, it is perceived that there is the factor of convenience. One of the interviewees gave an example of this convenience factor. The company offered secure and encrypted USB-drives as an alternative for ordinary USB-drives, but the adoption and use was lagging behind expectations. It turned out that the drives were, due to port restrictions, not usable on computers outside the company and thus not practical (e.g. for presentations). As a consequence people still preferred the use of standard USB-drives, because they had always worked well for them and were much less restrictive. Besides, the secure USB-drives were so wildly expensive that department managers did not accept many of the requests for the secure drives; they were already on a tight budget, and did not see the added value of the USB- drives in relation to the price.

Concluding from this, we can state that the insurers see "security awareness" as at least an equally important factor to attain InfoSec goals as the security policies and technological solutions are. According to all interviewees security awareness is currently at the top of the priority list regarding InfoSec, although in some organizations still in an initial professionalization stage.

Key insights:

- The insurers state that their current maturity level on the basis of the DNB InfoSec program is 3, and they are working on reaching level 4.
- Smaller organizations may struggle to comply due to lack of resources and power, while the larger organizations struggle as a result of architectural complexity and legacy in their IT landscape.
- Employees sometimes ignore policies or security measures out of their self-confidence of the ability to keep data safe or out of convenience, as in the case of the encrypted USB-sticks.
- Security awareness is as such a bare necessity for organizations that process sensitive personal data.

Current Information Security and Risk Management Practices

When it comes to the topic of information security and risk management all interviewees were quite open in the description of the measures deployed to achieve security. As described above, one of the managers indicated that a high degree of security from external threats can be reached when proper technological measures are implemented. Besides, the IT management activities such as timely patching, Identity & Access Management and zero-day response are indicated as a key measure to keep data safe. Most organizations indicated to have a properly managed and implemented Identity and Access Management policy with role-based access control and, physical and logical, access restrictions.

In all organizations, the information security policies that govern the InfoSec capability in the organization are documented and fairly complete. Yet no insight gained on the communication and the knowledge regarding these policies in the organizations. With respect to risk management all health insurers indicated that, as prescribed by the DNB, the NOREA framework is used to analyze and categorize risk. However, regarding the Privacy Impact Analysis one of the interviewees indicated that the NOREA framework was impractical to implement. This organization was, as such, considering best-practices to construct an effective and compliant PIA framework. At all organizations the risk analyzes are periodically revised to keep insights in risks up-to-date, and be able to act quickly.

Regarding the measurement of actual InfoSec maturity and compliance with regulations, some health insurers indicated that a control framework had been implemented to effectively measure performance indicators for security. On the other hand there were also health insurers for which it cost an enormous effort in terms of time and resources to indicate and justify compliance. This may depend on both the degree of compliance of the organization, and the complexity of the organization and its processes.

As indicated earlier, all interviewees see security awareness as a big step towards attaining and maintaining full compliance. However, in several of the organization security awareness programs had only recently been initiated. Most organizations used e-learning programs and awareness sessions to increase awareness. On this topic all organizations indicated that top management involvement in training sessions, and in InfoSec in general, is key to promote the feel for necessity of awareness among employees.

Key insights:

- All (visited) insurers have high-maturity InfoSec policies in place, and mostly attain at least maturity level 3.
- Insurers state that implementation of technological measures can achieve a great deal of Information Security, but human actions are much harder to manage.
- All insurers execute thorough risk management procedures regarding InfoSec in their processes and systems, following NOREA frameworks and/or best-practices.
- Security awareness is seen as a big step in the aim for a higher maturity level.

Data Governance

In addition to the InfoSec interviews, we had the chance to conduct an interview exclusively on a Data Governance (DG) program at one of the insurers. Data governance is defined as follows by Khatri & Brown (2010, p. 149):

> *"data governance refers to who holds the decision rights and is held accountable for an organization's decision-making about its data assets"*

Khatri & Brown (2010, p. 149) distinguish five interrelated domains for DG, notably: data principles, data quality, metadata, data access, and data lifecycle.

DG is thus intended to structure the approach to data management throughout the organization in order to derive at a more efficient use of data, and to improve traceability of data streams and individual data items.

The project at the specific organization was sparked by the need to comply with Solvency II, and the EU Privacy Act, but also came out of a need from the business to more efficiently manage and use data throughout the organization. According to the interviewee the concept EU Privacy Act was taken into account from the start of the project and the company is planning to reach maturity level 3 on Data Governance in 2014.

The interviewee indicated that the data governance program includes InfoSec, but is much broader than that alone. DG is about "who is allowed to do what with which data and why", while InfoSec is about "how do we keep outsiders and unauthorized persons away from the data". As explained by the interviewee the difference in approach between DG and InfoSec lies in the fact that InfoSec is implemented from the IT side of the organization, and is as such imposed on the business, while DG is implemented from the business side.

In the project the organization considered numerous best-practices and combined the best and most applicable parts into a Data Governance program for the organization. The resulting DG capability helps the organization to appropriately share data internally, trace data streams throughout the company and its third-party relationships, protect information (incl. personal data of clients) from unauthorized disclosure, and stay in compliance with privacy regulations.

Regarding the data, the organization made a selection of Corporate Data Objects that have been divided into numerous data vaults with individual security keys. The data is split-up in a way that renders the contents of a data vault useless for an intruder. If someone manages to get in he needs to get information from at least several vaults to get only a very narrow insight, while at that moment he is probably already compromised.

Because DG focusses on the business side, the program gives significant attention to the human factor in information management and security. Role-based access rights are taken into account in the program, and there is considerable attention for security awareness. In addition, the organization uses pattern-analysis to track errors and fraud, and as part of the program adjusts the limits of the data perimeter to only a small and select group of third-parties.

7. Conclusions & Recommendations

In this chapter we will conclude this research with respect to the research questions, and derive from that the recommendations for health insurers. In addition, we will provide a discussion and give suggestions for an alternative research methodology, and for future research into the subject of Information Security at health insurers.

7.1. Conclusions

In this section on the conclusions of this research we will firstly conclude on the findings from the interviews. After that, with the knowledge from the literature study and the interviews we will try to answer the research questions. Finally, we will try to formulate the main conclusions that can be stated on the basis of this research.

7.1.1. Conclusions from interviews

Based on the results and knowledge derived from the five interviews we can firstly state that all health insurers that were interviewed are properly informed on the GDPR, and that all are actively seeking ways in which compliance to the regulation now and in the future can be achieved. The organizations indicated that they have significantly professionalized their InfoSec capability in recent years (roughly since 2010). This was both as a response to the DNB Information Security program and out of their own vision on the necessity of InfoSec sparked by the consciousness that they could no longer depend on trust in the awareness of employees and an ad-hoc approach to security measures. From their own perception, the insurers have a maturity level of at least 3 at this moment in time, and an aim for maturity level 4 in the short run.

Although the insurers we visited did not struggle to implement measures to attain compliance with the DPA, they did indicate a struggle with the requirements of the GDPR. There are several potentially influential requirements in the GDPR. Regarding the justification of activities and the indication of effectiveness of measures, one of the insurers indicated that this impacts the organizations significantly due to the extra (human) resources for documentation and audit functions. On the right to be erased/forgotten, all insurers indicated that they expect an enormous impact as a result of both legacy in the IT landscape, and the number of third-parties that the insurers share data with. The main problem here is that data has to be traceable, since the data of one specific person in the systems of both the insurer and the involved third parties has to be removed. This would be particularly difficult for older data from the period that data management was less developed.

With regard to the quality of the InfoSec policy and the actual execution of it, two organizations indicated that gaps between policy and practice existed and caused vulnerabilities in processes. In the first case data was disclosed without the proper signature on an official document, while in the second case ordinary USB-drives were used instead of the prescribed special USB-drives with encryption. The two main reasons for these policy/practice gaps were 1) convenience (e.g. the data had to be disclosed quickly as a consequence of haste, and the ordinary USB-drives were more convenient in case they needed to be used in presentations outside the company), and 2) tight (IT) budget (e.g. the special USB-drives were too expensive in relation to their operational value according to department managers on a tight budget).

Regarding organizational culture and values, the interviewees indicated that awareness of the sensitivity of data is in the veins of the organization, and as such the awareness of the necessity for security measures is very high. However, the fact that many financial institutions, including health insurers, had significant problems with regard to InfoSec in 2010 indicates otherwise. From the interviews we perceived that the security managers at the insurers see security awareness as a very important factor for a good Information Security function, since it concerns the human factor. The human factor is one of the central parts of Information Security that cannot completely be taken care of through technological measures, while it is extremely influential in practice. At all insurers I visited, awareness programs have been initiated at this moment. All insurers indicated that the involvement of (top) management in security awareness, but also in security as a whole, is seen as key to influencing the human factor in the organization.

7.1.2. Conclusions on research questions

Based on the literature study and the interviews we will attempt answer the main research questions that were posed in Chapter 1 in this section.

1. *What is the current status of privacy security at Dutch health insurers?*

As perceived from the interviews, the maturity on Information Security is currently about level 3 out of 5, and is still improving significantly. The fact that the organization we interviewed attain maturity level 3 means that they have formalized their InfoSec policies and measures and that they are working on making the effects of measures quantifiable and hereby more manageable. With regard to incidents on a yearly basis none of the health insurers indicated a severe breach in recent years except for one case which was widely discussed in Dutch media. None of the companies can indicate the impact of a possible breach in practice, and as such we cannot make a statement on that subject.

2. *What impact will the new EU and Dutch privacy laws and regulations have on health insurers?*

As found in recent reports on the changes in privacy regulations, and as perceived from the interviews the impact of the changes will be significant. The fact that all measures and processes have to be justified through documentation causes a significant workload for the organizations. Besides, the right to be forgotten is expected to have a very high impact since the execution requires extensive and professional data management at the level of the individual, which is nearly impossible for organizations with customer bases of hundreds of thousands to millions of people. The instruments that the law gives to the regulators mainly consist of pressure mechanisms on board level and monetary sanctions.

Severe punishment in case of non-compliance through high monetary sanctions is not impossible but unlikely since information security and privacy is a very high priority at practically all insurers. Although many organizations struggle to comply they all put significant effort into the improvement of information security.

3. *How does the current state of privacy security compare to the situation desired in the privacy laws and regulations?*

From the interviews it is perceived that the current state of information security corresponds to the maturity required in the Dutch DPA. In addition, the maturity levels corresponds with the higher requirements posed by the DNB in the InfoSec program. However, with regard to the GDPR we perceive from the interviews that insurers still have to take some significant steps with to make InfoSec justifiable and measureable. Currently, most insurers assess their state of information security through the controls that the DNB requires them to implement.

4. *How can health insurers practically improve their state of privacy security and become compliant to the privacy regulations?*

Because of a limited insight in the actual measures that health insurers deploy it is very hard to give suggestions for concrete improvements that would make organizations compliant to privacy regulations. More so because it is hard to determine the measures required for the GDPR. However, we can state that a very important measure towards Information Security is the execution and maintenance of security awareness programs, and the top management support for these programs (not only through words but also through deeds). All organizations have already implemented, or are currently working on, security awareness programs.

A second measure for the longer term that we can suggest based on this research is a data governance program, in which access and distribution rights on data are properly determined, and data disclosure to internal and external parties is properly authorized and registered. Such a program would increase the ability to fulfill the right to be forgotten request, and most likely contribute to the effective use of organizational resources.

7.1.3. Final conclusions

On the basis of the literature study and the interviews at three health insurers we can argue that the state of Information Security has significantly improved in the past three to four years, and is perceived to be at maturity level 3 or higher at this moment. However, since we have not interviewed a sufficient number of organizations (5 to 6 out of 8) this statement cannot be generalized for the whole health insurance market.

On the basis of literature, research reports and common sense we can argue that it might well be that some of the smaller organizations still have significant difficulty to comply with both the DPA and with the DNB's Information Security requirements. Since for the smaller organizations the regulatory requirements set the same, very high targets for both the large (>10% market share) and the small (<5% market share) organizations. However, it is exactly that group of organization that we miss in this research.

As perceived from the interviews, the main problems that health insurers deal with regarding the European General Data Protection Regulation are:

1. the extensive justification requirements that oblige organizations to document and justify every process, risk, mitigation, et cetera, in order to justify the "in control" state. This is expected to be a very resource intensive activity.
2. the execution of the right to be erased/forgotten. This requirement requires very detailed management of data, on the level of the individual, to trace data of an individual through the organization and related third-parties. The organization has to be able to indicate internally and to third-parties with which data was shared, that the records of a requesting individual should be erased.
3. the threat of high monetary sanctions resulting from data breaches and incompliance.

In the pursuance of InfoSec most organizations follow ISO, COBIT and/or comparable standards and guidelines for the design and implementation of security measures and processes. In addition, we found that when the guidelines provided by ISO or ISACA/NOREA do not give a suitable solution, organization will look for it in other best-practices guidelines. Based on standards, guidelines and best-practices all insurers have developed information security policies, and implemented a broad range of measures and IT controls on the level of applications, databases, networks, et cetera. These controls include network compartmentalization, firewalls, Identity & Access Management processes, et cetera, and enable the organizations to protect personal (health) data from internal and external threats.

However important these InfoSec policies and technology enabled security measures are to achieve a high maturity level, the organizations all indicated that proper management of the human factor is the ultimate key to achieving proper Information Security at a health insurance organization. This finding was expected and is widely supported by literature and best-practices. However, the proper management of the human factor is a complicated issue that depends of many factors, as follows from the Technology Acceptance Model literature. Factors include both the cultural values of the organization, and the knowledge level of the employee. In addition, there should be a sense of urgency for the employee, which can at least partially, be created through top management involvement and the cultural values in the business with regard to InfoSec.

7.2. Recommendations

On the basis of this research we can define several recommendations to the health insurers, but also to other relevant actors related to the health insurers and privacy regulations, namely 1) the DNB as supervisor for the Dutch financial services industry, 2) the CBP and the European privacy supervisors on the WBP and the future GDPR, and 3) the European Commission that develops and approves the GDPR. Therefore, we firstly set out some recommendations for the last group in section 7.2.1 before we give recommendations for the health insurers themselves in section 7.2.2.

7.2.1. Recommendations for actors related to health insurers and privacy regulations

De Nederlandsche Bank

Based on the interviews and the results we found in this research we want(ed) to make the statement that the DNB should renew its analytical framework and the circular on Information Security. The findings from the 2010 benchmark are clearly outdated as perceived from this research, and in addition the health insurers indicated that the DNB should renew the analytical framework to include COBIT 5 controls since the 2010 framework was based on the older version COBIT 4.1. The insurers indicated that they ran into compatibility problems since they already made, or wanted to make, a switch to COBIT 5. However, we recently discovered that during the execution of this research the analytical framework has been updated to a 2014 version that takes into account COBIT 5 and includes two additional guidelines for Information Security. These two guidelines are the "SANS Top 20 Critical Security Controls for Effective Cyber Defense" and the "ISO 27032:2012 Guidelines for Cyber Security" (De Nederlandsche Bank, 2014c). Then what still misses is the release of an updated circular with respect to the current problems in the financial services industry, and the improvements that have been achieved in the past four years.

CBP & EU Privacy supervisor

To the CBP and the European supervisor on the GDPR we want to recommend to take into account the difficulties that organizations have to deal with concerning the practical implementation of a high-impact regulation such as the GDPR. Therefore we would suggest to provide clear and practical guidelines to guide organizations to compliance. In the current situation organizations regularly struggle to reach compliance, partially because of the vagueness of law texts and the generality of standards and guidelines.

European Commission

The last party besides the health insurers to which we want to make recommendations is the European Commission, the party that will eventually propose and agree on the final version of the European Privacy Act of which the GDPR is a part. This recommendation regards the targeting of the regulation, which is now unified for all data processing organizations that are active on the European market (which is also one of the spear points of the regulation). However, there is an important distinction between several sorts of personal data processing organizations. Some parties, such as social media platforms, see the gathering and marketing of personal data in exchange for a service to the customer as their primary process. While organizations such as health insurers process data to provide a service that benefits the customer him/herself and are not intended to violate his/her privacy in any sense. The consequence is that requirements intended to restrict privacy impacting activities also significantly impact organizations that are intended to keep private data safe and private. Therefore we recommend to differentiate between at least those two types of organizations to increase the fairness of the regulation.

7.2.2. Recommendations for improving information security at health insurers

There are numerous recommendations that we want to make to health insurers for the improvement of their InfoSec capability. These not only regard the improvement of InfoSec maturity, but also the improvement of the efficient execution of measures with regard to use of organizational resources.

Firstly, it is apparent that IT budget does not in itself increase maturity of effectiveness, the budget provides a financial resource that has to be put to the most effective use in 1) technological measures (Information Security and Privacy Enhancing Technologies), 2) process design and organizational measures (Privacy by Design/Default), and 3) security awareness enhancement.

Mostly with regard to the last category, but also for security measures in general, Beautement, Sasse, & Wonham (2009) argue that the effectiveness of InfoSec and security awareness programs depends to a large degree on a second type of budget, the “compliance budget” of employees. Beautement et al. (2009) state that an employee has a certain threshold, a budget. Above this budget the request for an extra effort to be invested in complying with organizational (security) policies adds nearly zero effectiveness, and may even work counterproductive. As a consequence of this intrinsic budget, the organization should not overfeed its people with security measures and awareness programs, but should: 1) aim to embed security in the organization’s culture and the employee’s values and practices, and 2) aim to reduce the impact of security measures on the employee daily work practices by taking into account the practical execution during the development and testing of the measure.

Both these measures work to increase the more effective use of the financial budget since the embedding of InfoSec into culture reduces the need for security awareness programs. While on the other hand the cooperation between the business and IT in the development of measures increases the applicability of measures and reduced the impact on an employee’s activities through which it increases productivity.

Another recommendation regarding the effective use of organizational resources for both InfoSec and other organizational purposes is the initiation of a Data Governance program. The aim of a DG program should be:

1. the more effective use of organizational data sources;
2. an increased insight in data flows in the organization and to/from its third-parties, and;
3. the approach of InfoSec from the business side instead of the traditional IT side.

The benefits from the first point are apparent, the more effective use of data sources may enable a more accurate prediction of future healthcare use/cost, and the more effective execution of contracts with health providers. An example of a benefit from the second point is that the increased insight in data streams empowers the organization in the efficient and compliant execution of the Right of Insight and the Right to be Forgotten/Erased. The fact that DG views InfoSec from the business side enables the organization to develop more effective measures with less impact on the business, and in addition may increase the awareness of the necessity of measures since they now also come from the business side of the organization.

In addition to the effective use of the budget, there is a measure that is more related to InfoSec in practice, which is the responsibility for InfoSec and risk management in the organization. The responsibility for InfoSec should be clearly appointed and communicated in the organization, and the responsible person should carry out his responsibility to provide an example for his subordinates and act as a point of contact for notifications or complaints.

Although an organization can already reach a significant degree of security with technological measures we have not made any recommendations with regard to this type of measures. The opinion among insurers is that an organization should simply follow the latest best-practices with regard to technological measures, and implement those effectively. On the point of implementation, however, the human factor requires significantly more attention in the form of change management and security awareness. Therefore, according to the TAM model, the focus should be on top management involvement, organizational culture, and the sense of urgency and necessity of security measures. Again, here, security awareness and organizational culture are included in the recommendation.

In the following final recommendation the focus is on security awareness once again. At one of the health insurers, an issue on the measurability of security awareness programs to reduce the risk of social engineering kept returning. The organization indicated that both the risk and practical impact of social engineering and the mitigating effect resulting from security awareness cannot be measured. However, we may have found a solution to attempt to measure both which is derived from the practices of penetration testing or ethical hacking; social engineering penetration testing on the call-center, preferably before and after security awareness training. In this way an organization can measure both the number and impacts of social engineering attempts that were successful, and in a second iteration after the program the impact of the security awareness training. Possible limitations of this approach are that 1) the “ethical engineers” may not be able to simulate the actual social engineering situation, that 2) because of the law an employer should maybe inform employees of the test, which will influence their behavior, and that 3) the increased telephone traffic on the call-center may go at the cost of regular clients.

7.3. Discussion

In this discussion section we present the view of the author/researcher on the conclusions from this research, the credibility of this research and we present suggestions for future research on the subject of Information Security at health insurers. Besides, we will also extend this research by offering an alternative research approach as a compensation for the low response on the requests for interviews at health insurers, and the low response on the request to fill the analytical framework. This alternative method concerns a Delphi-study, of which a concept version is given in the appendices.

7.3.1. Credibility of research

Regarding the credibility of this research we can state that the literature research is sound while with respect to data collection it is just sufficient considering the sensitivity of the subject, although could have been better due to several factors that we have summed up here. Firstly, in the research methodology the sensitivity of the subject Information Security was not taken sufficiently into account. As a consequence we have only gained access to three out of the eight health insurers. In addition, we had anticipated on the fact that the interviewees would be willing to give insight in the maturity of their InfoSec capability by completing the analytical framework. Again, the main problem here is the sensitivity of the subject that was not taken into account. As such, too little data was collected to be analyzable with statistical tools such as SPSS, as was intended. (Grimm, 2010)

The small research group and the lack of both qualitative and quantitative data, especially of the smaller insurance organizations, may have resulted in several biases. Firstly, have to deal with the social desirability bias, which may result in the interviewees sketching a too bright picture (keeping up appearances) of InfoSec in the interviews. Secondly, the actual overall state of InfoSec may be much worse than stated in this research since there is little insight in the organizations we did not interview, which may have rejected the request because of the suboptimal state of InfoSec.

A factor that influences the credibility of the analysis of the DPA and GDPR lies in the fact that the researcher is not a law student but a business student. As such, the researcher did not have much experience with reading and analyzing law texts. For this piece of research this was an essential part of the project, since one of the main subjects was the brand new GDPR. The fact that it is a relatively new regulation which is not yet accepted officially, means that there is no insight in actual cases and there is very little research on possible impacts. Luckily support was given by a lawyer, Judith Vieberink of First Lawyers, who is specialized in privacy laws and the Dutch DPA.

7.3.2. Contribution to science and suggestions for future research

In this piece of research we have made several contributions to science regarding Information Security at health insurers, and regarding the General Data Protection Regulation. Firstly, we developed, on a more practical than scientific basis, an analytical framework for the analysis of Information Security specifically at health insurers. In the first place, the framework has to be more thoroughly tested and justified through a larger sample of organizations and feedback by users. When the accuracy of the framework is confirmed, it can, through future research, possibly be generalized or simplified to increase the applicability to a broader range of (financial) organizations.

Secondly, this thesis provides one of the first comprehensive scientific and practical insights in the impact of the GDPR on a group of organizations on which the regulation is likely to have a deep impact. Again, though, this insight must be further tested and elaborated on, preferably both from the side of law science and the side of the business.

7.3.3. Alternative research approach

Since in this research we did not manage to achieve a sufficient amount of data to provide definitive answers to support the conclusions we can conclude that the research approach was not appropriate for investigating Information Security at health insurers. Therefore, we suggest an alternative approach that, with the experiences gained here, may result in the collection of sufficient data.

A central problem in the approach of the research population was the fact that InfoSec is a sensitive topic, about which security managers in general do not want to talk with unknown parties. The consequences of leaking sensitive information in an interview may be significant for the organization(s), e.g. negative media attention, loss of trust among clients, et cetera.

Although anonymity in the research was guaranteed in the interviews, an interview in itself is not absolutely anonymous since the interviewer knows the interviewee. This fact may initially lead to a reluctance to cooperate, and secondarily to biases in the interview results. A way to mitigate these risks related to interviews is to make the data collection process truly anonymous. This can most likely be achieved by using a survey, for example based on the Delphi method.

The Delphi method, named after the “Oracle of Delphi”, is a so-called structured communication technique in which a panel of experts individually and anonymously answers a questionnaire on a certain subject, after which the results are processed and distributed to all participants. The questionnaire generally consists of statements that the participant has to judge. Considering the statements in the InfoSec analysis framework, and the questions in the interviews the Delphi method seems to be a suitable alternative method of data collection for this research. The results of the questionnaire would be much more structured and analyzable than the current interview results, and it would provide a much more anonymous questionnaire environment for the research population.

However, although a Delphi study gives several advantages over the current research approach with regard to data collection, anonymity and analyzability of results, there are also several pitfalls to it. Firstly, there is still no guarantee that the targeted persons actually fill in the question list. Secondly, it is not verifiable that the person with the right qualifications (e.g. Security officer/CIO) that was actually targeted for the research has filled in the online survey. The third pitfall is that, as with the interviews, there is no way of verifying that a person truthfully fills in the answers. A fourth and final pitfall is that in contrast to an interview, which generally takes an hour, an online survey cannot take too long because of the attention span of the person who has to answer the questions.

Execution of a Delphi study

On the internet numerous tools can be found through which anonymous web questionnaires can be made, and communicated to a research population. The survey tool offered by SurveyMonkey.com, for example, provides settings through which e-mail and IP address tracking can be disabled to guarantee anonymity to a high degree. For this research, such a tool would be adequate to conduct a Delphi study.

As an example of what such a Delphi study should look like for this research we have constructed a draft survey in Google Forms, which can be found in Appendix D – Delphi study survey form. To take into account the attention span limit of 15 minutes, and to take into account both the interview and the analytical framework in the web survey we have taken questions and statements from both sources. In the first section of the survey we set out to identify the position of the filer, categorize the organization, and determine the focus on privacy regulations which we also do in the interviews. The second section takes the nine categories in which we have subdivided all answers to the statements in the analytical framework, and pose five to ten statements from the framework for every category. In this way we derive at a small subset of the analytical framework with which we are to a certain degree able to determine the maturity and construct a spider diagram of it comparable to the analytical framework.

Since the execution period for this research is limited to five to seven months at most, the execution of a questionnaire based on the Delphi is not achievable. However, the Delphi method should be taken into account when further research into the topic of Information Security is conducted in a sensitive environment such as the health insurance sector, where anonymity is key for the collection of a satisfactory amount of trustworthy data.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Ajzen, I., & Fishbein, M. (1970). The prediction of behavior from attitudinal and normative variables. *Journal of Experimental Social Psychology*, *6*(4), 466–487.

Albrecht, J. P. (2013, October 17). General Data Protection Regulation in 10 Points. Retrieved from http://www.janalbrecht.eu/fileadmin/material/Dokumente/131016_Data_protection_press_briefing_final_Engl.pdf

Aramis Jeanpierre. (2013, December 20). Meldplicht datalekken en Meldplicht inbreuken op elektronische systemen. Retrieved August 26, 2014, from http://www.cip-overheid.nl/wp-content/uploads/2013/12/Meldplicht-092.pdf

Baveco, M. P. P., & Bikker, H. (2011, November 24). Circular on Information Security. De Nederlandsche Bank. Retrieved from http://www.toezicht.dnb.nl/en/binaries/51-224608.pdf

Beautement, A., Sasse, M. A., & Wonham, M. (2009). The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 workshop on New security paradigms* (pp. 47–58). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1595684

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices. *USF Tampa Library Open Access Textbooks Collection*. Retrieved from http://scholarcommons.usf.edu/oa_textbooks/3

Carbonel, J.-C. (2008). Assessing IT Security Governance Through a Maturity Model and the Definition of a Governance Profile. Retrieved April 4, 2014, from http://www.isaca.org/Journal/Past-Issues/2008/Volume-2/Pages/Assessing-IT-Security-Governance-Through-a-Maturity-Model-and-the-Definition-of-a-Governance-Profile1.aspx

CMMI Product Team. (2010). CMMI for Services, version 1.3. Carnegie Mellon, Software Engineering Institute. Retrieved from http://repository.cmu.edu/sei/286/

College Bescherming Persoonsgegevens. (2013, February). CBP Richtsnoeren: Beveiliging van Persoonsgegevens. College Bescherming Persoonsgegevens. Retrieved from http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

Council of Europe. (n.d.). Personal Data Protection Act (Unofficial Translation). Council of Europe. Retrieved from http://www.coe.int/t/dghl/standardsetting/dataprotection/national%20laws/NL_DP_LAW.pdf

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, *35*(8), 982–1003.

De Nederlandsche Bank. (2013, January). DNB Supervisory Themes 2013. De Nederlandsche Bank. Retrieved from http://www.dnb.nl/en/binaries/284483_DNB%20Supervisory%20Themes%202013.pdf

De Nederlandsche Bank. (2014a, January). DNB Supervisory Themes 2014. De Nederlandsche Bank. Retrieved from http://www.dnb.nl/en/binaries/304577_Thema%20uk.pdf

De Nederlandsche Bank. (2014b, May 22). Toelichting op Toetsingskader Informatiebeveiliging 2014. De Nederlandsche Bank. Retrieved from http://www.toezicht.dnb.nl/binaries/50-230767.pdf

De Nederlandsche Bank. (2014c, June 5). Information on 2014 Assessment Framework for Information Security (unofficial translation). De Nederlandsche Bank. Retrieved from http://www.toezicht.dnb.nl/en/binaries/51-230767.pdf

Duthler Associates. (2014, April 1). Europese richtlijn bescherming persoonsgegevens (95/46/EG) [Text]. Retrieved August 25, 2014, from http://www.duthler.nl/nl/europese-richtlijn-bescherming-persoonsgegevens-9546eg

Duthler, A.-W., & Biesheuvel, A. J. (2013, February). Het Europees privacyrecht in beweging: Overzicht van actuele ontwikkelingen en mogelijke consequenties voor werkzaamheden van IT-auditors. NOREA. Retrieved from http://www.surf.nl/binaries/content/assets/surf/en/2013/het-europees-privacyrecht-in-beweging_bw_v2.1.pdf

ENISA. (2013, November 12). ENISA Threat Landscape 2013 - Overview of current and emerging cyber-threats [Report/Study]. Retrieved February 8, 2015, from https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

European Parliament. (2013, October 22). General Data Protection Regulation: Inoffical consolidated version after Libe committee vote. Jan Albrecht. Retrieved from http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf

European Parliament. (2014, April 3). Q&A on EU data protection reform. Retrieved August 25, 2014, from http://www.europarl.europa.eu/news/en/news-room/content/20130502bkg07917

Grimm, P. (2010). Social desirability bias. *Wiley International Encyclopedia of Marketing*. Retrieved from http://onlinelibrary.wiley.com/doi/10.1002/9781444316568.wiem02057/full

Infosecurity Magazine. (2014, July 3). Declaratiegegevens van 27.000 VGZ-verzekerden toegankelijk via internet. Retrieved August 1, 2014, from http://infosecuritymagazine.nl/2014/07/03/declaratiegegevens-van-27-000-vgz-verzekerden-toegankelijk-via-internet/

ISACA. (2009). An Introduction to the Business Model for Information Security. ISACA. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf

ISACA. (2014). COBIT 4.1: Framework for IT Governance and Control. Retrieved September 18, 2014, from http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

ISO/IEC. (2013). ISO/IEC 27001:2013. ISO/IEC. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=54534

Johnson, A. M. (2005). The Technology Acceptance Model and the Decision to Invest in Information Security (pp. 114–118). Presented at the Proceedings of the 2005 Southern Association of Information Systems Conference, Southern Association of Information Systems. Retrieved from http://sais.aisnet.org/2005/Johnson.pdf

Jones, C. M., McCarthy, R. V., Halawi, L., & Mujtaba, B. (2010). Utilizing the Technology Acceptance Model to Assess the Employee Adoption of Information Systems Security Measures. *Issues in Information Systems*, *1*(11), 9–16.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly*, 183–213.

Khatri, V., & Brown, C. V. (2010). Designing Data Governance. *Commun. ACM*, *53*(1), 148–152. http://doi.org/10.1145/1629175.1629210

Kiely, L., & Benzel, T. (2006). Systemic Security Management: A new conceptual framework for understanding the issues, inviting dialogue and debate, and identifying future research needs. U.S. Marshall School of Business. Retrieved from http://www-marshall.usc.edu/assets/004/5347.pdf

Mettler, T., & Rohner, P. (2009). Situational maturity models as instrumental artifacts for organizational design. In *Proceedings of the 4th international conference on design science research in information systems and technology* (p. 22). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1555649

Ministerie van Veiligheid en Justitie. Wet Bescherming Persoonsgegevens, Internet § 1 (2000). Retrieved from http://wetten.overheid.nl/BWBR0011468/Hoofdstuk1/Artikel1/geldigheidsdatum_30-06-2014

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, *2*(3), 192–222.

Moormann, J., & Schmidt, G. (2006). *IT in der Finanzbranche: Management und Methoden*. Heidelberg: Springer Verlag.

Nederlandse Zorgautoriteit. (2009, July). Vervolgonderzoek privacy bij zorgverzekeraars: Opvolging van verbeterpunten. Nederlandse Zorgautoriteit. Retrieved from http://www.nza.nl/104107/138040/Rapport-vervolgonderzoek-privacy-bij-zorgverzekeraars.pdf

Nederlandse Zorgautoriteit. (2013, September). Marktscan en beleidsbrief Zorgverzekeringsmarkt: Weergave van de markt 2009-2013. Nederlandse Zorgautoriteit. Retrieved from http://www.nza.nl/104107/105773/742312/Marktscan_en_beleidsbrief_Zorgverzekeringsmarkt_2013.pdf

Ponemon Institute. (2013, May). 2013 Cost of Data Breach Study: Global Analysis. Ponemon Institute/Symantec. Retrieved from https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

Robles, R. J., Choi, M., Cho, S.-E., Lee, Y., & Kim, T. (2009). SOX and its effects on IT Security Governance. *International Journal of Smart Home*, *3*(1), 81–87.

Roessing, R. von, & Information Systems Audit and Control Association. (2010). *The Business Model for Information Security*. Rolling Meadows, IL: ISACA. Retrieved from http://www.books24x7.com/marc.asp?bookid=39949

Staten-Generaal, T. K. der. (1998, March 2). Wet bescherming persoonsgegevens; Memorie van toelichting [officiële publicatie]. Retrieved August 25, 2014, from https://zoek.officielebekendmakingen.nl/kst-25892-3.html

Van Hillegersberg, J. (2013, June). *Information Systems in the Financial Services Industry - lecture 1: Introduction to the course*. Lecture, Enschede.

Venkatesh, V., & Bala, H. (2013). TAM 3: Advancing the technology acceptance model with a focus on interventions. *Manuscript in Preparation. Retrieved from Http://www. Vvenkatesh. com/IT/organizations/Theoretical_Models. Asp# Utaut*.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management Science*, *46*(2), 186–204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425–478.

Verizon. (2013, April 22). 2013 Data Breach Investigations Report. Verizon Enterprise Solutions. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Verizon. (2014, April 21). 2014 Data Breach Investigations Report. Verizon Enterprise Solutions. Retrieved from http://www.verizonenterprise.com/DBIR/2014/

Wang, P. A. (2010). Information security knowledge and behavior: An adapted model of technology acceptance. In *2010 2nd International Conference on Education Technology and Computer (ICETC)* (Vol. 2, pp. V2–364–V2–367). IEEE. http://doi.org/10.1109/ICETC.2010.5529366

Appendices

Appendix A – List of abbreviations

APT – Advanced Persistent Threat
BMIS – Business Model for Information Security
CBP – College Bescherming Persoonsgegevens
CIA – Confidentiality, Integrity & Availability
CIO – Chief Information Officer
CISO – Chief Information Security Officer
COBIT – Control Objectives for Information Related Technology'
CvZ – College voor Zorgverzekeringen (from 2014 on Zorginstituut Nederland (ZIN))
DDOS – Distributed Denial of Service
DG – Data Governance
DMZ – De-militarized Zone
DNB – De Nederlandsche Bank
DPA – Data Protection Act
DPO – Data Protection Officer (Dutch: functionaris gegevensbescherming)
DTC – Diagnosis Treatment Combination (Dutch: diagnosebehandelingscombinatie)
FSA – Financial Services Act
FSI – Financial Services Industry
GDPR – General Data Protection Regulation (EU)
IAM – Identity & Access Management
IDS – Intrusion Detection System
ICIIP – University of Southern California's Institute for Critical Information Infrastructure Protection
InfoSec – Information Security
ISACA - Information Systems Audit and Control Association
ISMS – Information Security Management System
ITIL – Information Technology Infrastructure Library
NOREA - Nederlandse Orde van Register EDP-Auditors (EN: Dutch order of Registered EDP-Auditors) (Dutch chapter of ISACA)
NZa – Dutch Healthcare Authority
PET – Privacy Enhancing Technologies
PIA – Privacy Impact Analysis
RBAC – Role-based Access Control
TAM – Technology Acceptance Model
WBP – Wet Bescherming Persoonsgegevens (= DPA)

Appendix B – Structured literature research

In this research we address several subjects with very broad fields of scientific research, namely IT Governance, Information Security, Information management, European privacy laws and regulation, and Identity & Access Management (as a broad subfield of Information security). In addition we have included the field of cyber-crime science, notably crime prevention, as was proposed by one of the project supervisors because it is a field that combines both crime science and information security. WE will discuss here the way in which the structured literature review was executed for every of these fields of research. Since the literature regarding cyber-crime science was provided by the supervisor we have not carried out a further literature research into that subject.

Information security

- *including refinement with words: maturity, model, management*

Search engines/scientific database: Google Scholar, Scopus, Web of Science

IAM

Search engines/scientific database: Google Scholar, Scopus, Web of Science

IT Governance

Search engines/scientific database: Google Scholar, Scopus, Web of Science

Information management

Search engines/scientific database: Google Scholar, Scopus, Web of Science

European privacy laws and regulations

Sources: Eur Lex, Dutch lawbook, European lawbook

Appendix C – Structured interviews

Pre-interview requirements – all interviews

Before the interviews could be conducted most organizations posed several requirements for the handling of interview results and the guarantee of anonymity of the interviewees and their organizations. Since this also likely improved the quality of the answers the interviewees give I have agreed on the following requirements for before the interview started:

- I send the thesis report for review before publication;
- I shall not use the interviews for commercial purposes;
- I do not use information in my thesis, and in my research in general, that can lead to a specific organization, and ask the university if the thesis doesn't have to be publicly available. If else I will censure the results to guarantee anonymity;
- After the completion of this research I will send the thesis with the research results to all interviewees;
- If necessary I will sign a non-disclosure act with regard to the information that I have gathered about the organization.

Interview health insurers – information security problems and practices

General questions

- What is the size of the organization in terms of personnel?
- What percentage of the personnel is directly in contact with customer data for day-to-day work activities? (e.g. administration, call-center)
- What is the size of the organization in terms of customer base?

Questions for organization with more than one label

- Are the data streams and processing steps separated among the labels? If yes, to what degree and how?
- Is the InfoSec strategy and governance similar for all labels?
    - If it differs, how does it differ?
        - Differs on small agreements?
        - Differs greatly?
    - Where does the final responsibility regarding InfoSec lie, with the main organization or with the label?

Questions for all organizations

- How many incidents does the organization have on average in which the confidentiality of personal data is violated?
    - What is the impact for the organization?
    - What is the impact for the customer?
    - Where do these incidents originate from?
        - Human error by personnel?
        - (security) Awareness? (e.g. phishing, social engineering)
        - Fraud (from internal organization)?
        - Hacking?
- Related to the DPA

  - How aware is your organization of the DPA and the revisions in the DPA?
  - What do you think of the new fines related to the *Obligation to* report In case of a dataleak? (from €4500 to €450.000 in DPA, and in EU Privacy Act to €100 mln, or 5% of the worldwide turnover)
  - Do you think your organization complies to the current regulations?
    - To what degree?
  - Do you think your organization will be able to comply to the near-future revised regulations?
    - The Obligation to report
    - The “right to be forgotten”
    - Control over data to customer
  - Does the view on InfoSec in your organization change with the big change in the regulation?
    - How does it change?
      - IT/InfoSec budget?
      - More active approach?

Questions related to InfoSec

- Related to the InfoSec governance/policy
  - Is there a general InfoSec Strategy
    - Including IT/information lifecycle management
  - Is there a thorough risk management policy that includes
    - Official risk assessment guidelines
    - Periodic assessment
    - Privacy Impact Assessment
  - Are the governance/policy documents:
    - Well documented
    - Read throughout the organization
    - Known throughout the organization
    - Applied throughout the organization
- Related to human factors
  - Personnel is still a significant factor in the occurrence of InfoSec vulnerabilities, how do you tackle this problem?
    - Security awareness training
    - Control rules in applications
    - Policies on:
      - Clean desks
      - Use of paper and USB sticks
    - Regular random testing and inspection
- Related to crime science
  - How do you work on
    - i. increasing the effort it takes to execute a criminal activity
      - access and surveillance related InfoSec measures

        - ii. increasing the risk for a criminal of getting caught
            - Surveillance, monitoring, and security aware personnel?
        - iii. reducing the reward that results from the criminal activity
            - Network compartmentalizing, …
        - iv. reducing provocations that may lead people to carry out criminal behavior
            - Fair promotion and reward management
            - Fair management
            - Socially conscious investing (e.g. no child labor, no wasteful industries, no arms industry, no bio-industry)
            - Provide listening ear for whistleblower, act on vulnerability warnings by personnel
        - v. removing excuses that the criminal give as reasons for carrying out the criminal activity
            - Fair promotion and reward management
            - Fair management
            - Socially conscious investing (e.g. no child labor, no wasteful industries, no arms industry, no bio-industry)

Analytical framework

- I have built an analytical framework for InfoSec measures and policies based on:
    - ISACA COBIT 5 and BMIS (the Business Model for Information Security
    - CBP Privacy Guidelines
    - DNB Assessment Framework for Information Security
- Do you want to fill it in for your organization and send it back to me? It provides part of the justification of this research.

Interview health insurers – CIO high-level InfoSec view

Questions related to organization

- Does the organization have one or more labels?
    - If more than one, is the data processed separately?
        - To what degree are processes separated?
        - Is the Information Security strategy determined per label or for the organization as a whole?
            - Are there labels for which special arrangements with regard to security count?
        - Where are the final responsibilities for InfoSec, with the central organization or with the labels?
    - Is there enough control over de execution of the InfoSec strategy in the organization?
        - If more than one label; is there enough control over execution of the strategy at all labels?

General questions

- What is the opinion on InfoSec in the organization's Top Management?
    - Is there enough attention for the subject, and is this carried out in the organization?

- What do you think of the 2010 InfoSec program initiative from the DNB?
- Do you think that this initiative has had a strong influence on the current state of InfoSec at this organization?
    - What is the current state of InfoSec at this organization in terms of maturity level?
    - How does this state compare to the organization's maturity state of 2010?

- What measures does this organization take to keep up with the requirements the DNB states in her InfoSec program?

Changes in the privacy regulations, from DPA to European GDPR

- Are you up-to-date with the coming changes in the European privacy regulations and the GDPR?
    - Does the focus on InfoSec at this organization change as a consequence of the new regulations?
    - To what degree do you think this organization can take the right measures in time (around 2016) to comply with the regulation? (E.g. become "in control" with regard to processes and systems in which personal data is being processed)
    - To what degree do you think that the InfoSec program initiative has helped to get a grip on the InfoSec function in this organization?

- Compliance at this organization?
    - Does this organization currently comply with the DPA, and do you think this organization will be able to comply with the new regulation in time?
    - Is there an extensive program for periodic Risk Analysis, including a Privacy Impact Assessment, at this organization?
        - Is there a clear responsibility for the mitigation of risk that are known from risks analyses?
        - Is there knowledge of the analysis in the organization (readable and read?)
    - The Data Leak Notification directive requires the precise detection of a data leak, a quick response to limit the data loss, and the quick identification of the impact. What measures does this organization take to be able to fulfill these requirements in case of a data leak?

- How does this organization fulfill the Privacy by Design/Privacy by Default approach requirement in the development of applications and processes?

Questions with regard to InfoSec

- What is your opinion on the view of InfoSec as an "organizational capability" that has to be developed in the organization and has to mature over a longer period of time?
    - What factors do you think might have an important influence on the development of such a capability?
        - Strategy of the organization?
        - Structure of the organization?
        - Financial resources to bring the strategy into practice?
        - Knowledge and skills to bring the strategy into practice?
        - Determination and leadership to bring the strategy into practice?
        - Environmental factors, such as:
            - Competition in the sector?

            - Regulations?
            - The actual threat level

- What role do you see for IT Governance and Data Governance in attaining and maintaining compliance with privacy regulations?
    - What does this organization do on the subject of governance?
        - A general InfoSec strategy
        - IT/information life-cycle management
        - Data governance?
    - How does this organization make sure that the governance on paper is also put to practice, and has an actual impact on the maturity state of InfoSec?

- Human factors – employees form a great threat to the organization because mistakes are human. What does this organization do to minimize mistakes, and the impacts of mistakes made by personnel?

- Integrity – It is essential that all personal data about the customers is correct and stay correct in all processes and databases/vaults. There are several possible causes that may threaten integrity. How does this organization deal with this, what measures are taken?

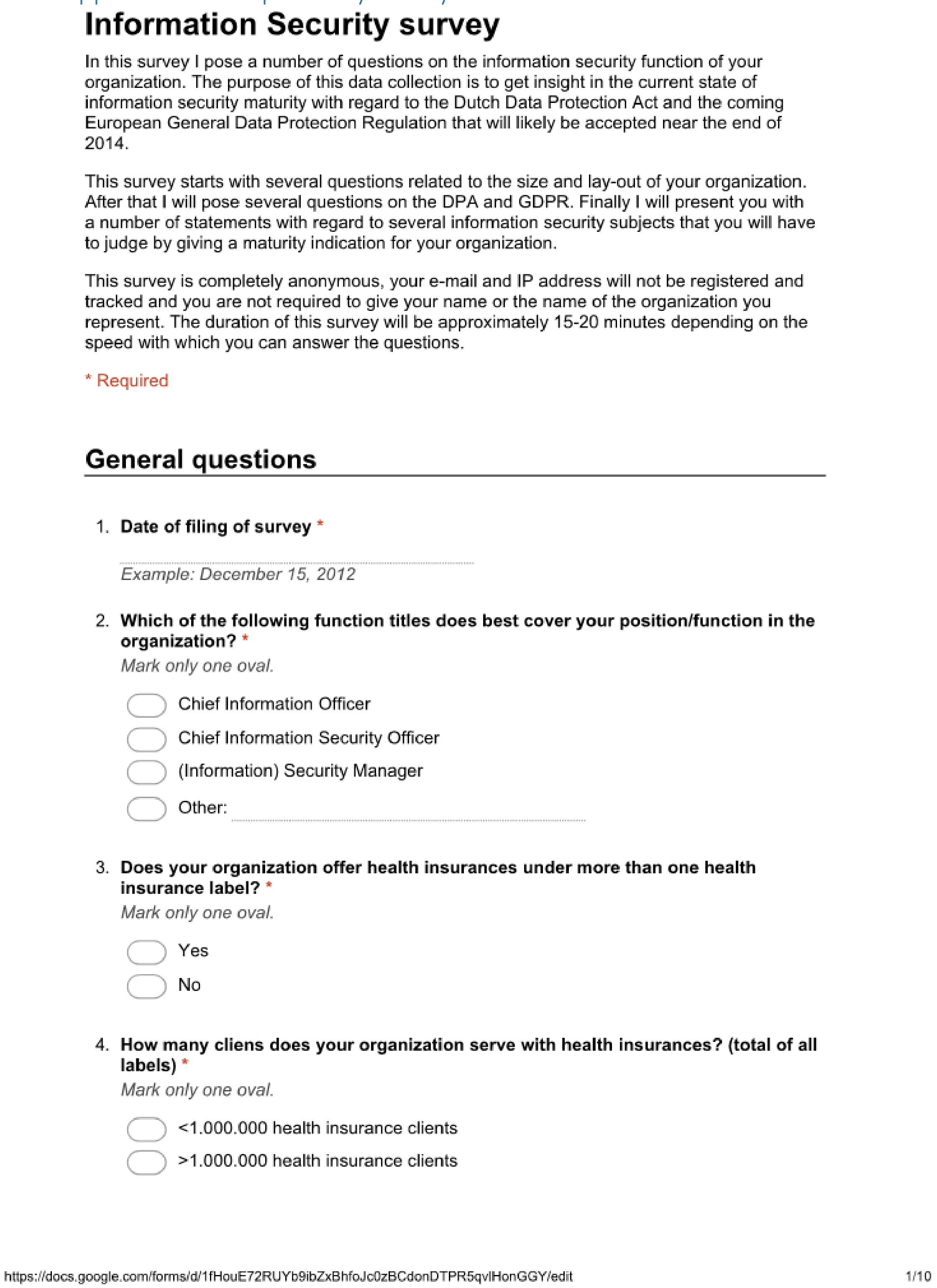
Interview health insurers – Data Governance Program

Interview

- How high is the awareness of the changes in the DPA and EU privacy regulations at this organization?
    - The law requires the quick and accurate detection of data leaks, and in response to that a quick notification that a data leak has occurred. How do you manage that at this organization?
    - The law requires the client to have access and rectification abilities on his/her own information, how do you manage this aspect in this organization?
    - Have you thoroughly documented all processes in which personal data is processed?
- How did this data governance (DG) program come about?
    - How long is the organization working on this project?
    - What has sparked the initiation of the program?
        - Necessity to make data management more efficient?
        - Has the program been initiated out of a necessity to be able to comply to the WBP or privacy regulations in general?
    - Have you used data governance standards for the composition of the DG policy, such as COBIT or ISO/IEC 38500?
    - Is the DG program part of the information security strategy?
        - If yes, to what degree?
- When the renewed WBP follows in a couple of years and when the client will get more control over his data, will the degree of access for the customer to data be determined on the basis van this program?
    - To what degree do you take the renewed regulation into account in this program?

- Will there be one policy for whole organization as a result of this program?
    - Is there a distinction between health insurance and other departments in the policy?
    - Is there a distinction between declaration data (DBC's) and name and address data + BSN in the policy? (how will the client be administered, on the basis of his/her BSN or policy number? How does this work for database normalization?)
- How many data sensitivity classification layers are there within the model that results from this program?
    - How do you classify/categorize data, on what basis?
        - On the basis of privacy (according to WBP & EU Privacy Act)?
        - On the basis of impact on the organization?
        - On the basis of sensitivity for the organization/the customer?
    - Wherein is the distinction between those layers?
        - Regarding handling of data by personnel and in systems?
            - Regarding access rights and RBAC
        - Regarding disposal of digital and paper information sources (also regarding old hard disks in old IT hardware)?
            - Is there, for example, a clause on e-waste in the policy?
        - Regarding storage at third-party, where is the organizational perimeter/barrier for data of a certain classification?
- Many data leaks emerge through human errors by personnel, how do you handle this threat?
    - To what degree does the possibility exist to extrude privacy sensitive data from a secure to an insecure environment, for example through USB-sticks, paper, Excel-files, etc.?
    - To what degree does the possibility exist to register human errors, and to prevent them from occurring? For example:
        - Control rules in applications
        - Random samples
        - Training/awareness sessions
        - Change log on data (old version can be reconstructed and person where error occurred can be traced)
- How does the organization enforce personnel to act according to the policy?
    - Through fines or threatening measures
    - Through awareness (creation)
    - Through hard-coded restrictions and access rights in applications

Appendix D – Delphi study survey form



Information Security survey

In this survey I pose a number of questions on the information security function of your organization. The purpose of this data collection is to get insight in the current state of information security maturity with regard to the Dutch Data Protection Act and the coming European General Data Protection Regulation that will likely be accepted near the end of 2014.

This survey starts with several questions related to the size and lay-out of your organization. After that I will pose several questions on the DPA and GDPR. Finally I will present you with a number of statements with regard to several information security subjects that you will have to judge by giving a maturity indication for your organization.

This survey is completely anonymous, your e-mail and IP address will not be registered and tracked and you are not required to give your name or the name of the organization you represent. The duration of this survey will be approximately 15-20 minutes depending on the speed with which you can answer the questions.

* Required

General questions

1. **Date of filing of survey** *

   ____

   Example: December 15, 2012

2. **Which of the following function titles does best cover your position/function in the organization?** *

   Mark only one oval.

   ○ Chief Information Officer

   ○ Chief Information Security Officer

   ○ (Information) Security Manager

   ○ Other: ____________________

3. **Does your organization offer health insurances under more than one health insurance label?** *

   Mark only one oval.

   ○ Yes

   ○ No

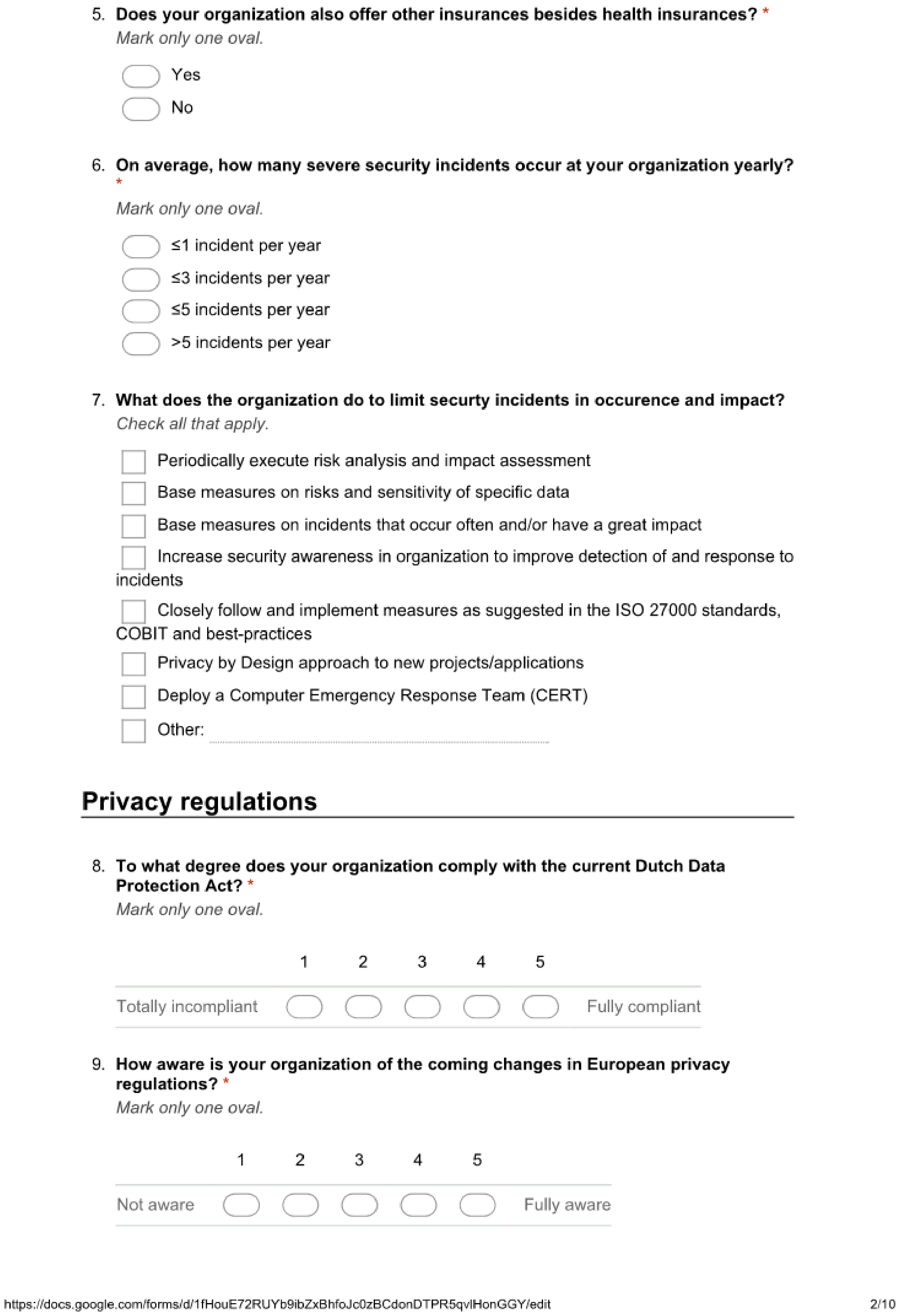
4. **How many cliens does your organization serve with health insurances? (total of all labels)** *

   Mark only one oval.

   ○ <1.000.000 health insurance clients

   ○ >1.000.000 health insurance clients

https://docs.google.com/forms/d/1fHouE72RUYb9ibZxBhfoJc0zBCdonDTPR5qvlHonGGY/edit 1/10



5. **Does your organization also offer other insurances besides health insurances?** *
Mark only one oval.

○ Yes
○ No

6. **On average, how many severe security incidents occur at your organization yearly?** *
Mark only one oval.

○ ≤1 incident per year
○ ≤3 incidents per year
○ ≤5 incidents per year
○ >5 incidents per year

7. **What does the organization do to limit securty incidents in occurence and impact?**
Check all that apply.

□ Periodically execute risk analysis and impact assessment
□ Base measures on risks and sensitivity of specific data
□ Base measures on incidents that occur often and/or have a great impact
□ Increase security awareness in organization to improve detection of and response to incidents
□ Closely follow and implement measures as suggested in the ISO 27000 standards, COBIT and best-practices
□ Privacy by Design approach to new projects/applications
□ Deploy a Computer Emergency Response Team (CERT)
□ Other: ____________________

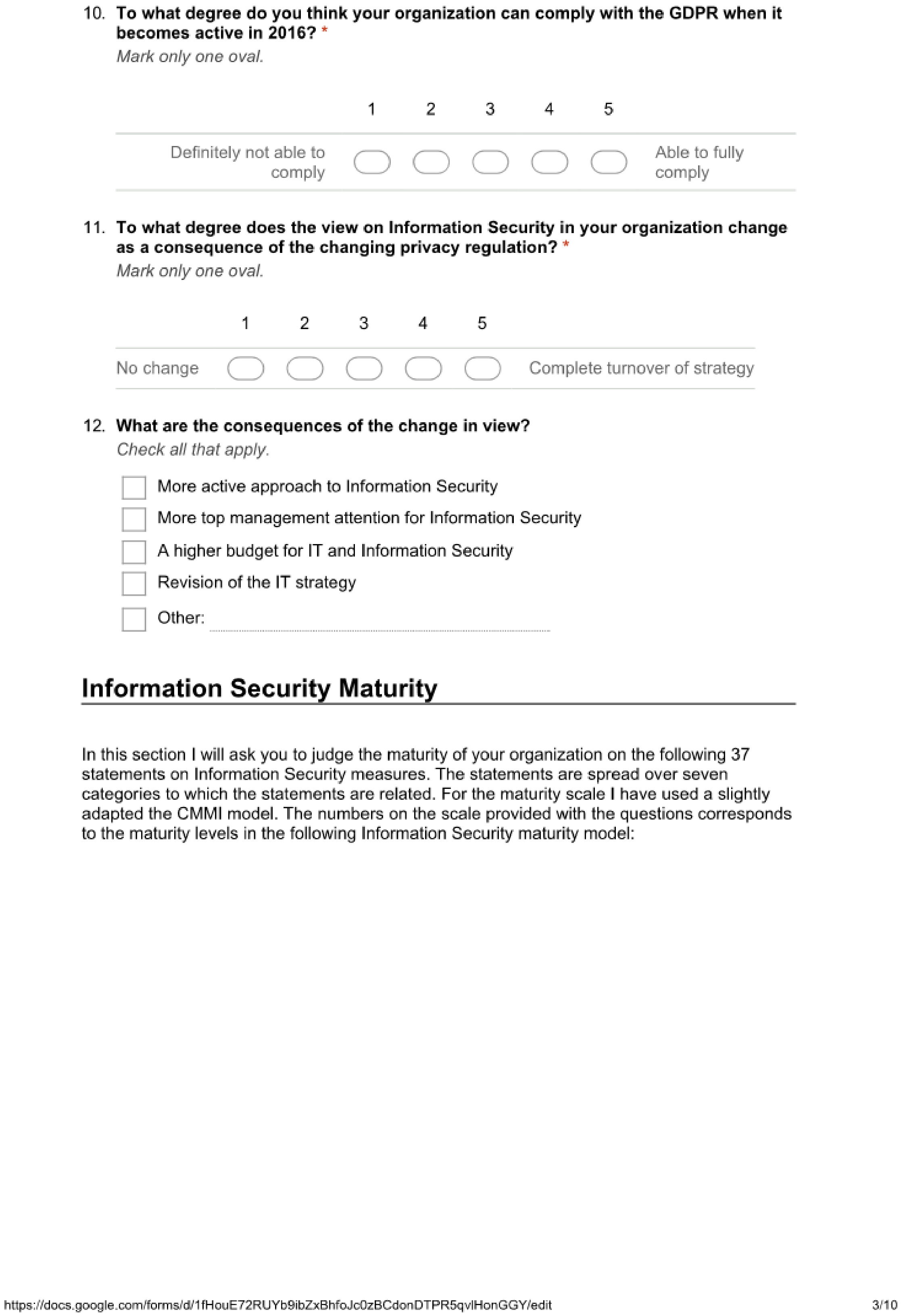
Privacy regulations

8. **To what degree does your organization comply with the current Dutch Data Protection Act?** *
Mark only one oval.

	1	2	3	4	5	
Totally incompliant	○	○	○	○	○	Fully compliant

9. **How aware is your organization of the coming changes in European privacy regulations?** *
Mark only one oval.

	1	2	3	4	5	
Not aware	○	○	○	○	○	Fully aware



10. **To what degree do you think your organization can comply with the GDPR when it becomes active in 2016?** *

Mark only one oval.

	1	2	3	4	5	
Definitely not able to comply	○	○	○	○	○	Able to fully comply

11. **To what degree does the view on Information Security in your organization change as a consequence of the changing privacy regulation?** *

Mark only one oval.

	1	2	3	4	5	
No change	○	○	○	○	○	Complete turnover of strategy

12. **What are the consequences of the change in view?**

Check all that apply.

□ More active approach to Information Security

□ More top management attention for Information Security

□ A higher budget for IT and Information Security

□ Revision of the IT strategy

□ Other: ____________________

Information Security Maturity

In this section I will ask you to judge the maturity of your organization on the following 37 statements on Information Security measures. The statements are spread over seven categories to which the statements are related. For the maturity scale I have used a slightly adapted the CMMI model. The numbers on the scale provided with the questions corresponds to the maturity levels in the following Information Security maturity model:

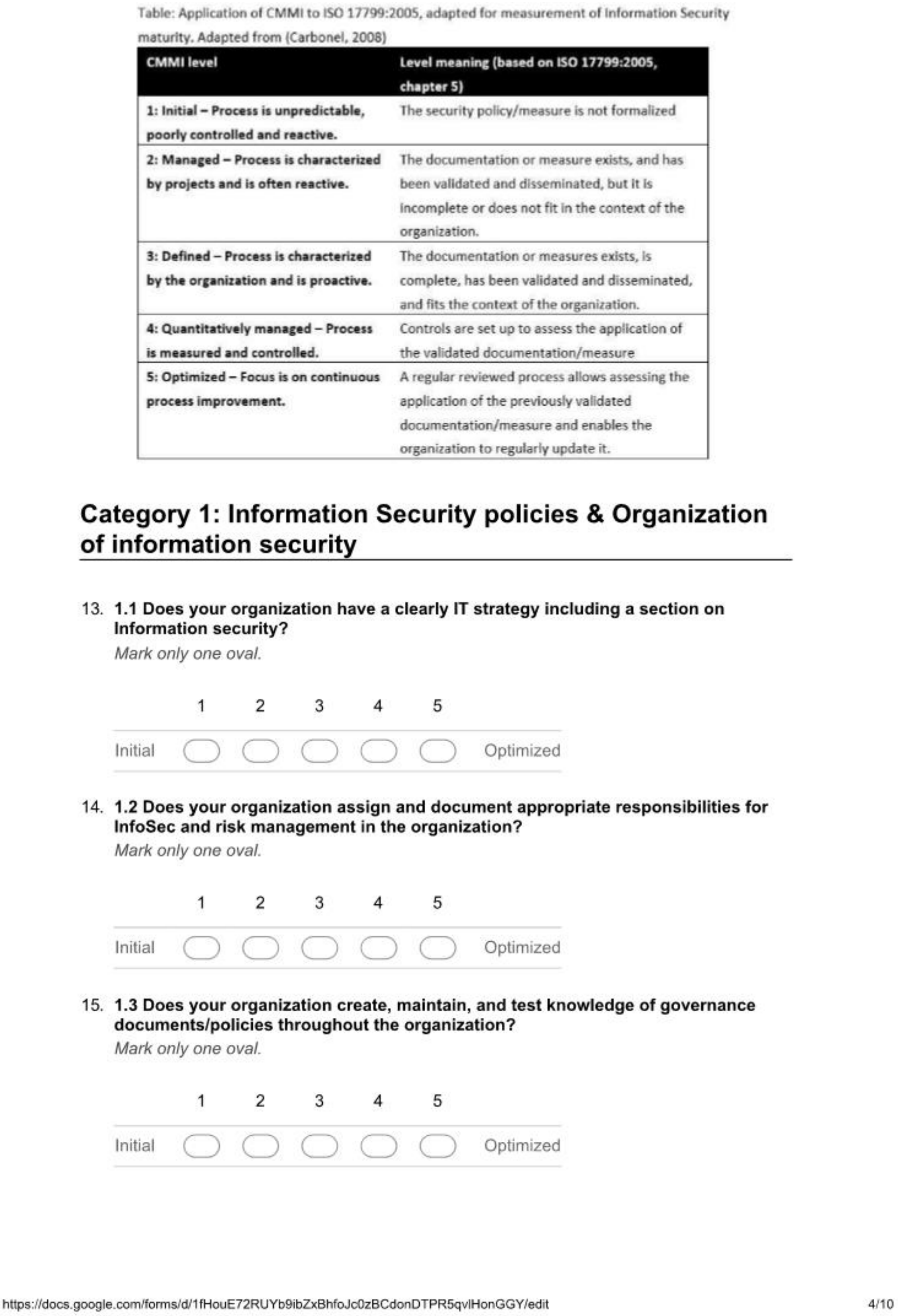


Table: Application of CMMI to ISO 17799:2005, adapted for measurement of Information Security maturity. Adapted from (Carbonel, 2008)

CMMI level	Level meaning (based on ISO 17799:2005, chapter 5)
1: Initial – Process is unpredictable, poorly controlled and reactive.	The security policy/measure is not formalized
2: Managed – Process is characterized by projects and is often reactive.	The documentation or measure exists, and has been validated and disseminated, but it is incomplete or does not fit in the context of the organization.
3: Defined – Process is characterized by the organization and is proactive.	The documentation or measures exists, is complete, has been validated and disseminated, and fits the context of the organization.
4: Quantitatively managed – Process is measured and controlled.	Controls are set up to assess the application of the validated documentation/measure
5: Optimized – Focus is on continuous process improvement.	A regular reviewed process allows assessing the application of the previously validated documentation/measure and enables the organization to regularly update it.

Category 1: Information Security policies & Organization of information security

13. **1.1 Does your organization have a clearly IT strategy including a section on Information security?**

Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

14. **1.2 Does your organization assign and document appropriate responsibilities for InfoSec and risk management in the organization?**

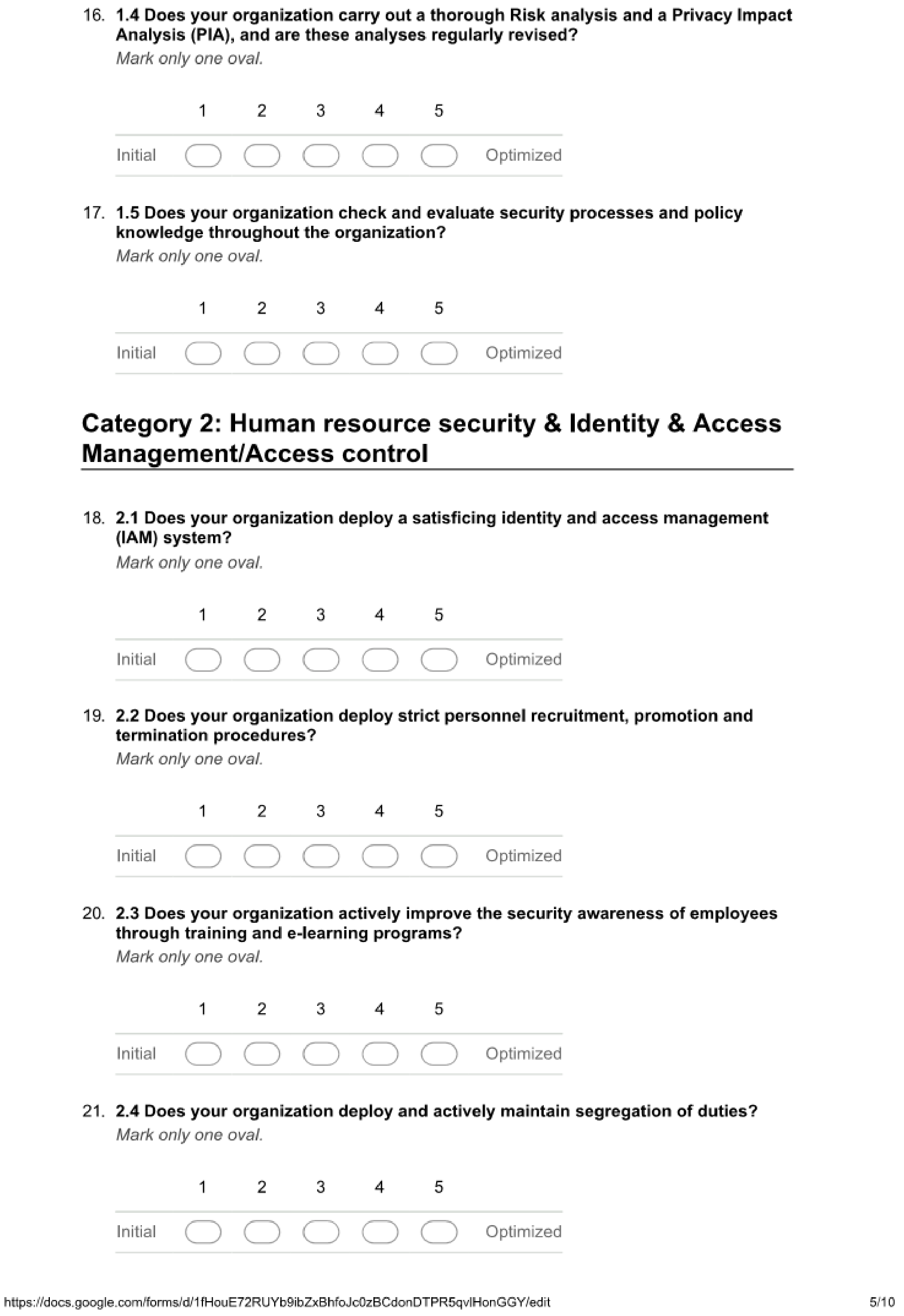
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

15. **1.3 Does your organization create, maintain, and test knowledge of governance documents/policies throughout the organization?**

Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized



16. **1.4 Does your organization carry out a thorough Risk analysis and a Privacy Impact Analysis (PIA), and are these analyses regularly revised?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

17. **1.5 Does your organization check and evaluate security processes and policy knowledge throughout the organization?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

Category 2: Human resource security & Identity & Access Management/Access control

18. **2.1 Does your organization deploy a satisficing identity and access management (IAM) system?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

19. **2.2 Does your organization deploy strict personnel recruitment, promotion and termination procedures?**
Mark only one oval.

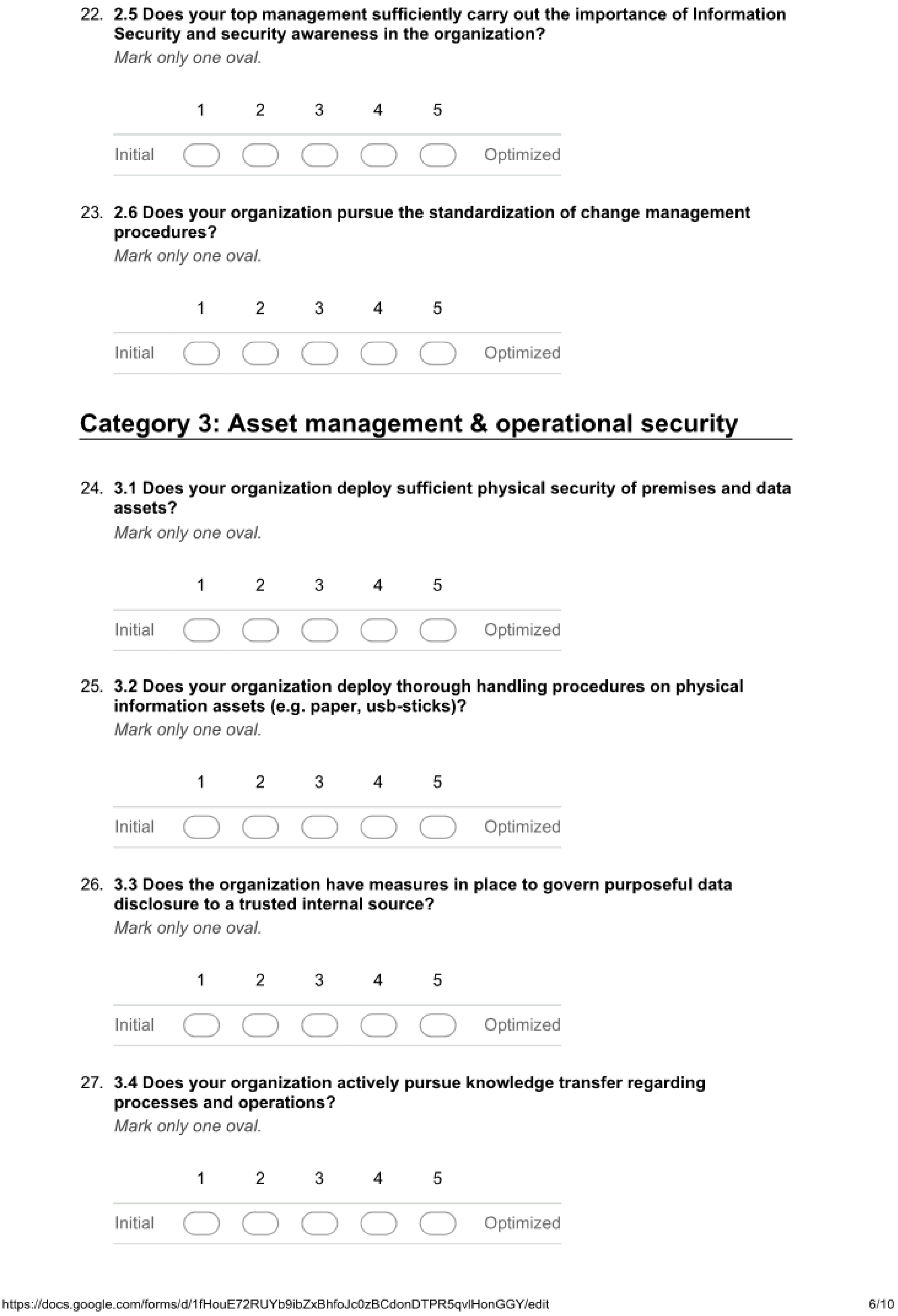
	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

20. **2.3 Does your organization actively improve the security awareness of employees through training and e-learning programs?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

21. **2.4 Does your organization deploy and actively maintain segregation of duties?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized



22. **2.5 Does your top management sufficiently carry out the importance of Information Security and security awareness in the organization?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

23. **2.6 Does your organization pursue the standardization of change management procedures?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

Category 3: Asset management & operational security

24. **3.1 Does your organization deploy sufficient physical security of premises and data assets?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

25. **3.2 Does your organization deploy thorough handling procedures on physical information assets (e.g. paper, usb-sticks)?**
Mark only one oval.

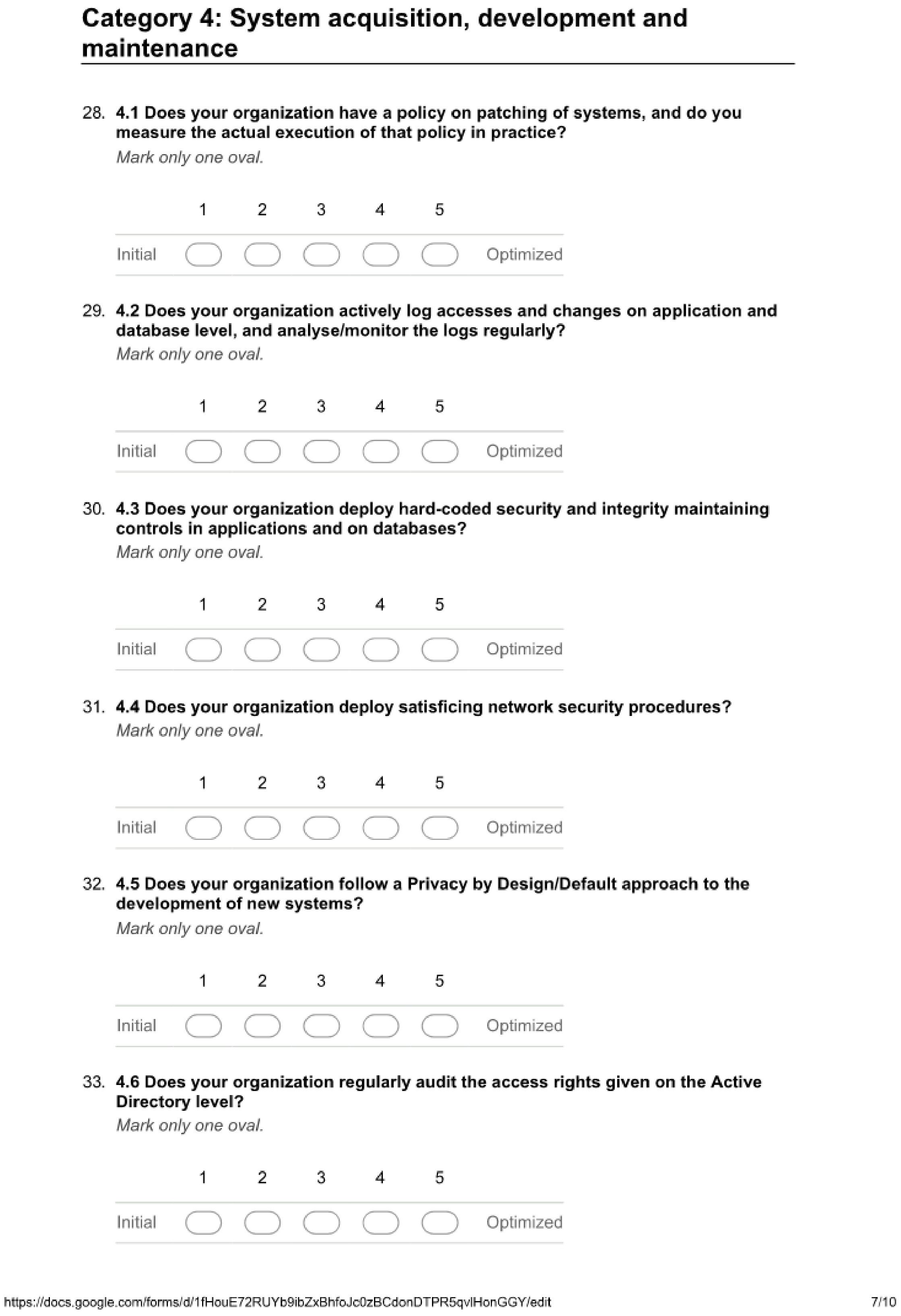
	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

26. **3.3 Does the organization have measures in place to govern purposeful data disclosure to a trusted internal source?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

27. **3.4 Does your organization actively pursue knowledge transfer regarding processes and operations?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized



Category 4: System acquisition, development and maintenance

28. **4.1 Does your organization have a policy on patching of systems, and do you measure the actual execution of that policy in practice?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

29. **4.2 Does your organization actively log accesses and changes on application and database level, and analyse/monitor the logs regularly?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

30. **4.3 Does your organization deploy hard-coded security and integrity maintaining controls in applications and on databases?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

31. **4.4 Does your organization deploy satisficing network security procedures?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

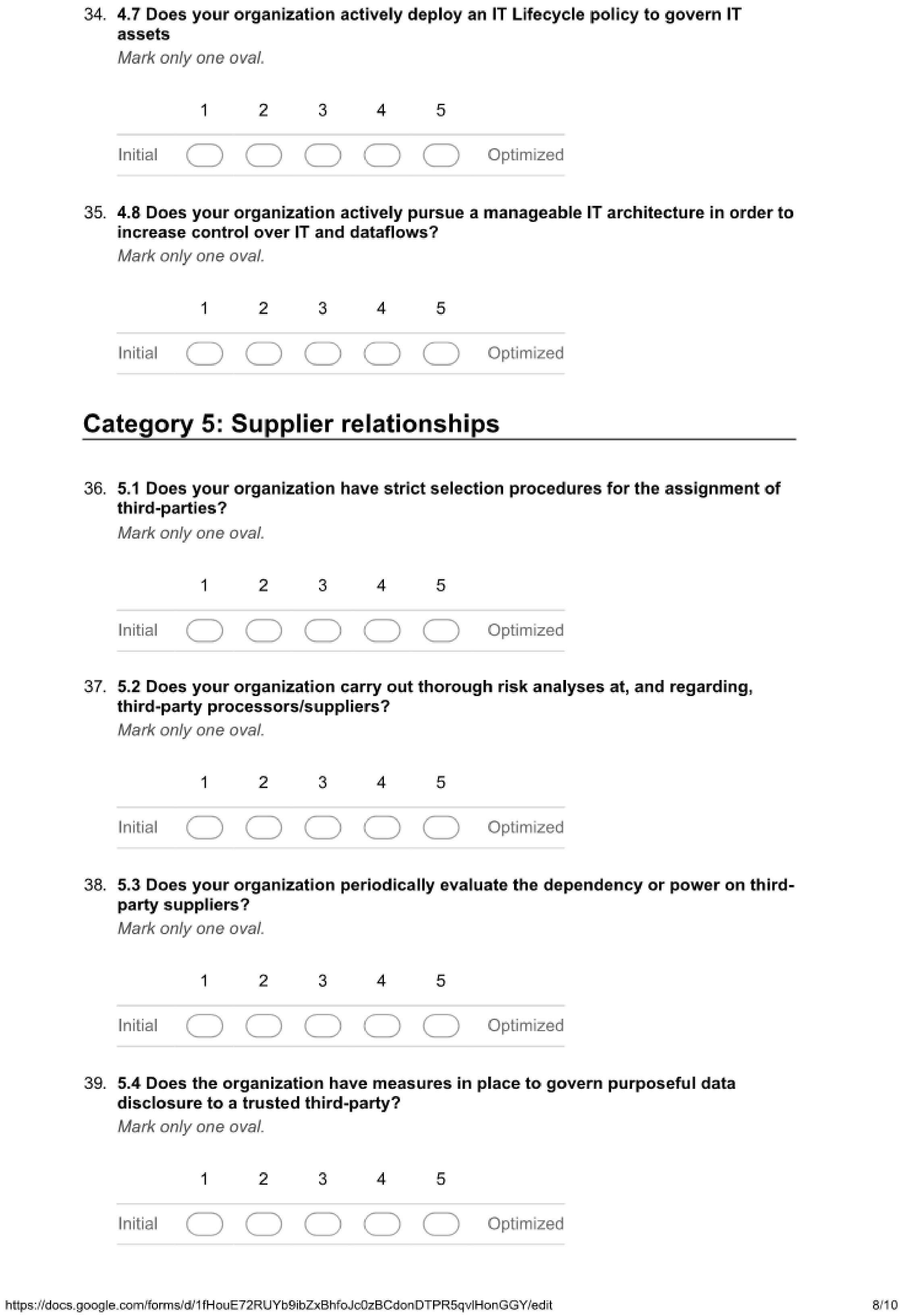
32. **4.5 Does your organization follow a Privacy by Design/Default approach to the development of new systems?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

33. **4.6 Does your organization regularly audit the access rights given on the Active Directory level?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

https://docs.google.com/forms/d/1fHouE72RUYb9ibZxBhfoJc0zBCdonDTPR5qvlHonGGY/edit 7/10



34. **4.7 Does your organization actively deploy an IT Lifecycle policy to govern IT assets**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

35. **4.8 Does your organization actively pursue a manageable IT architecture in order to increase control over IT and dataflows?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

Category 5: Supplier relationships

36. **5.1 Does your organization have strict selection procedures for the assignment of third-parties?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

37. **5.2 Does your organization carry out thorough risk analyses at, and regarding, third-party processors/suppliers?**
Mark only one oval.

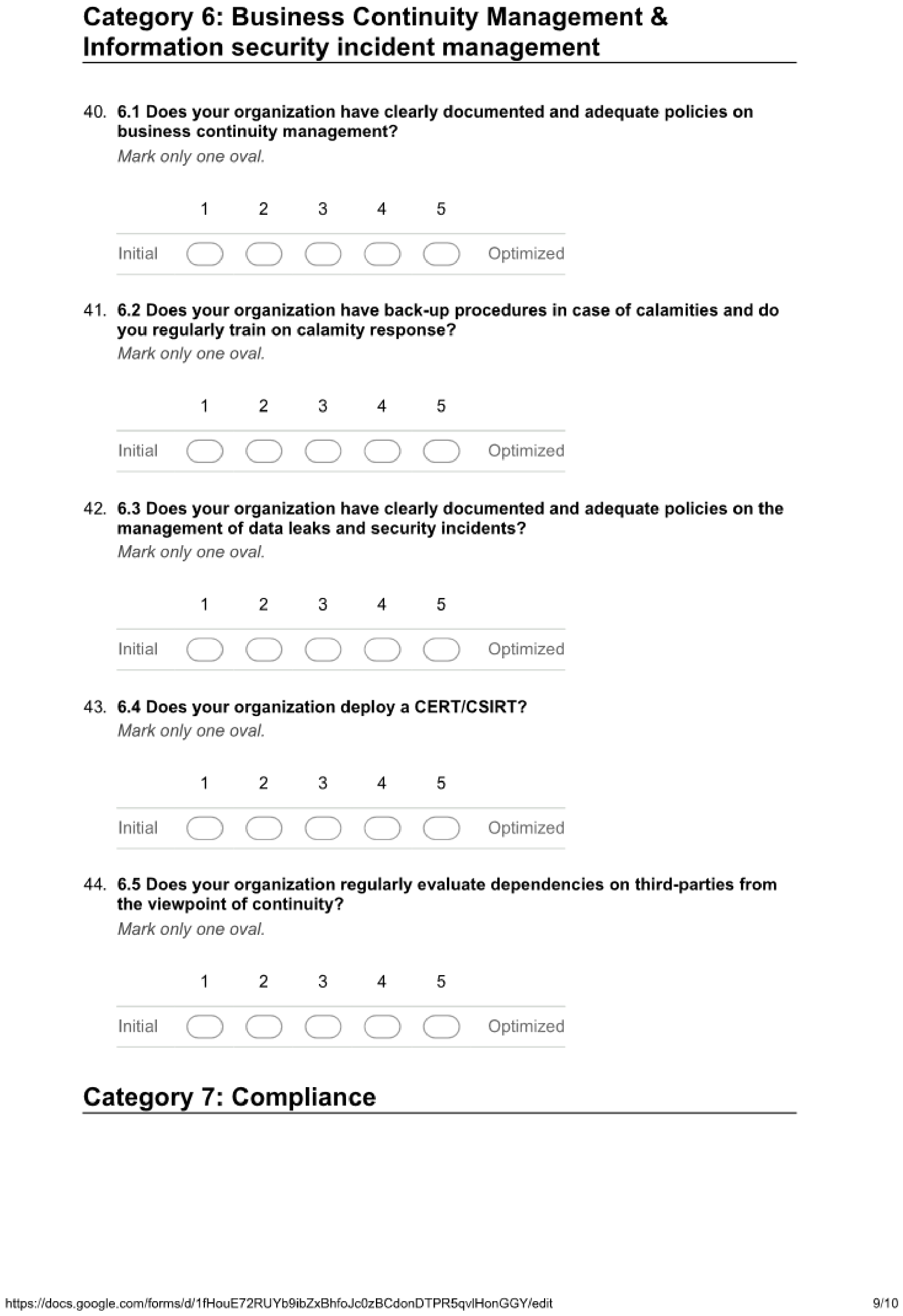
	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

38. **5.3 Does your organization periodically evaluate the dependency or power on third-party suppliers?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

39. **5.4 Does the organization have measures in place to govern purposeful data disclosure to a trusted third-party?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized



Category 6: Business Continuity Management & Information security incident management

40. **6.1 Does your organization have clearly documented and adequate policies on business continuity management?**

Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

41. **6.2 Does your organization have back-up procedures in case of calamities and do you regularly train on calamity response?**

Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

42. **6.3 Does your organization have clearly documented and adequate policies on the management of data leaks and security incidents?**

Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

43. **6.4 Does your organization deploy a CERT/CSIRT?**

Mark only one oval.

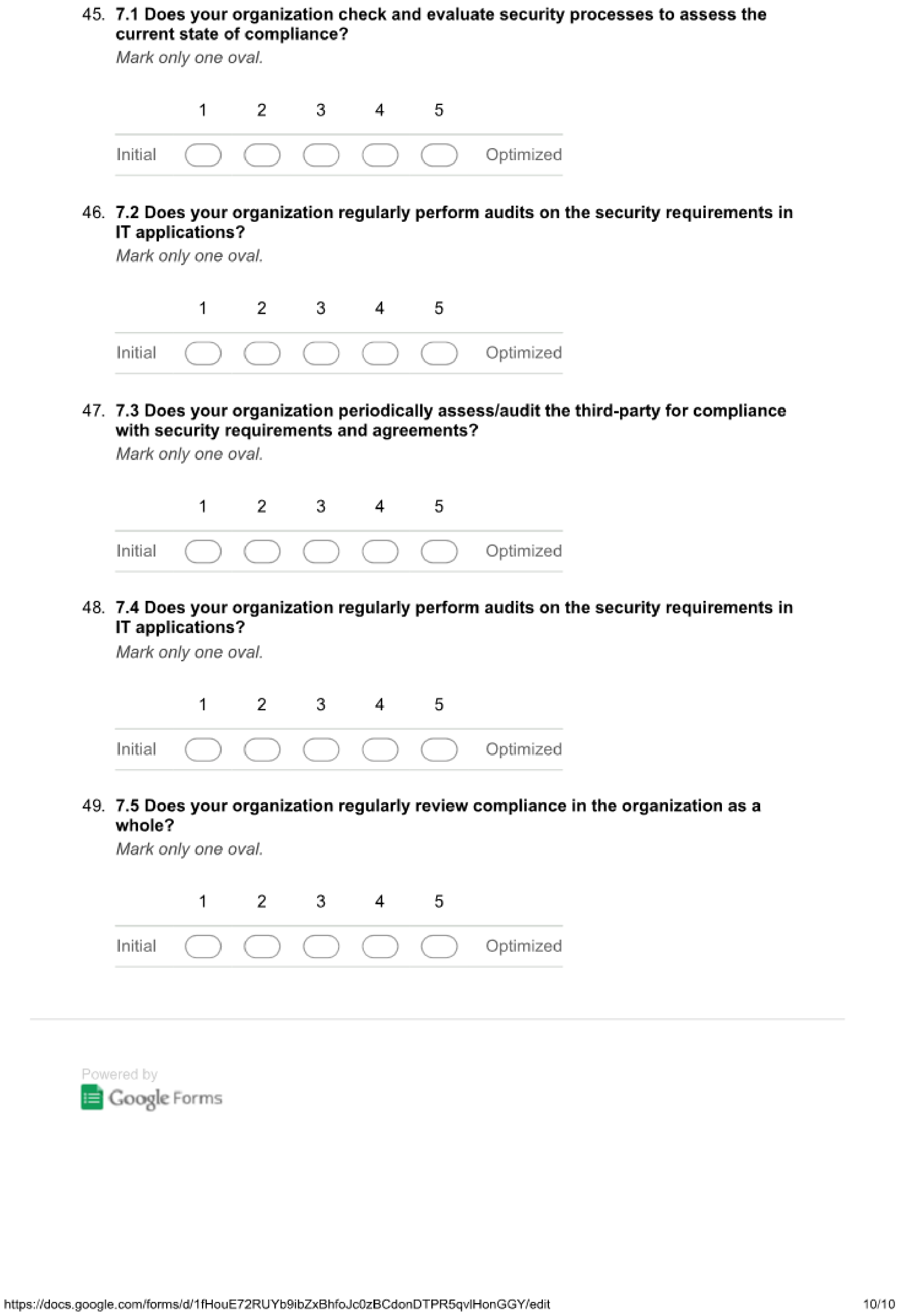
	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

44. **6.5 Does your organization regularly evaluate dependencies on third-parties from the viewpoint of continuity?**

Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

Category 7: Compliance



45. **7.1 Does your organization check and evaluate security processes to assess the current state of compliance?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

46. **7.2 Does your organization regularly perform audits on the security requirements in IT applications?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

47. **7.3 Does your organization periodically assess/audit the third-party for compliance with security requirements and agreements?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

48. **7.4 Does your organization regularly perform audits on the security requirements in IT applications?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

49. **7.5 Does your organization regularly review compliance in the organization as a whole?**
Mark only one oval.

	1	2	3	4	5	
Initial	○	○	○	○	○	Optimized

Powered by
Google Forms

https://docs.google.com/forms/d/1fHouE72RUYb9ibZxBhfoJc0zBCdonDTPR5qvlHonGGY/edit 10/10