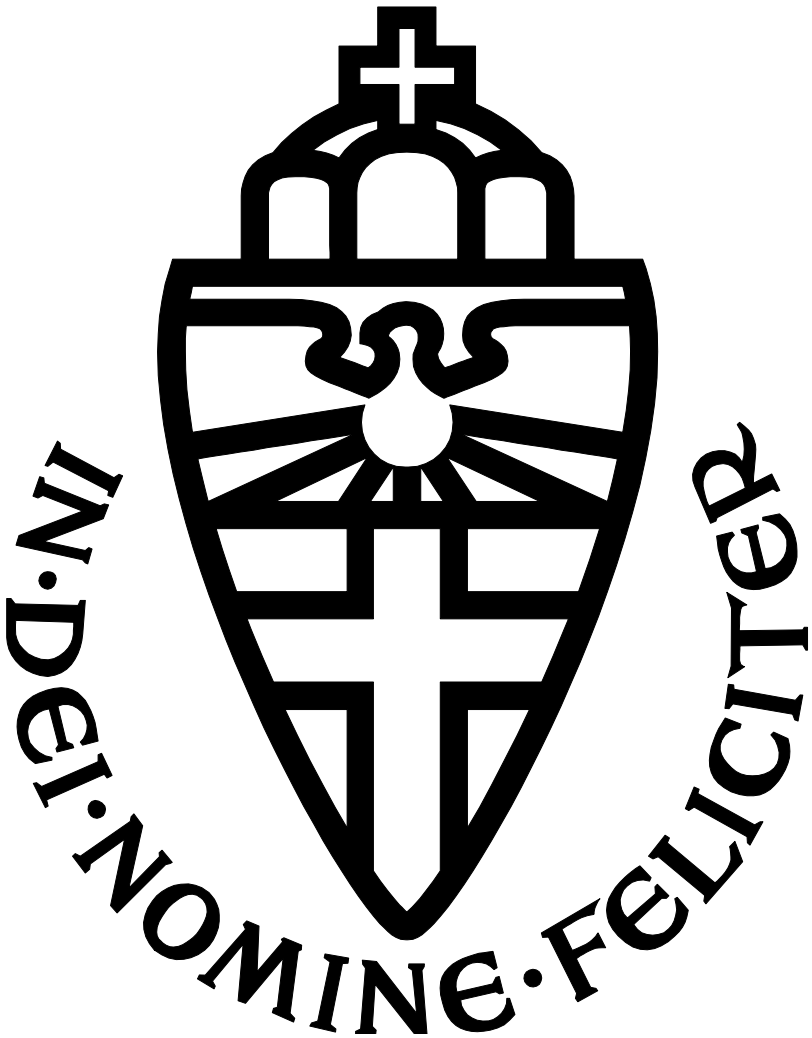
Information security in practice

The practice of using ISO 27002 in the public sector

By Pim Sewuster, s4009126
Supervised by Erik Poll
181 IK



Abstract

The objective of this thesis is to investigate what countermeasures for information security threats organizations typically use, and how they select such countermeasures.

To reach this goal, interviews were held with those in charge for their organization's information security. These interviews were two-fold: A set number of topics would be discussed. The topics are based on ISO 27002, the biggest standard for information security. These topics can then be used to compare organizations.

The other aspect of the interviews would be discussing how the organizations selected the counter-measures, and what they think is the best approach to selecting them.

Although many prescriptive documents on ISO 27002 exist, this research combines both previously named aspects into a descriptive overview of what controls typically are used, how they were selected and how the interviewed practitioners think they should be selected.

The two biggest issues found in this research were lack of management commitment and lack of employees' understanding of information security.

Acknowledgements

First and foremost, I would like to thank Erik Poll for helping me write this thesis; without his timely and accurate feedback I would not have succeeded.

Pieter Bokhoven, for helping me kick off this project. Because of him the scope of this project was defined well and quickly, and helped me immensely to get the thesis done within the normal timeframe.

Bert van den Brink and Jasper de Vries for spending time on helping me, despite of their busy scheduled. They helped me navigate through the vast knowledge network within Ernst&Young, giving me a lot of potential interviewees. Also, thanks to them for reviewing my documents whenever it was needed.

Finally I'd like to thank all the other colleagues at Ernst&Young for always being friendly and helpful.

Table of contents

Contents

1 Introduction

“Creating and implementing a proper information security program is not necessarily rocket science most of the important components that should be part of such a program are basically common sense. However, very often these common sense issues are ignored because there is a lack of understanding and realizing how essential they are” (von Solms & von Solms, 2004)

The quote above makes one wonder how organizations approach information security. Do they analyze what vulnerabilities their organization has, do they create ad-hoc solutions for perceived threats or do they do nothing at all?

Information is arguably the most important asset of most modern day companies, and protecting it should therefore be one of the core processes. However, higher management has more problems to worry about – and information security can be regarded as a Black Swan problem (Taleb, 2001). Black Swan problems are events that have a small chance of happening, with a big impact. Because of psychological biases, these problems are usually underestimated.

Information security is a Black Swan problem – even without spending a lot of resources, things could go right for a long time. For management, this can mean that they’re spending money on information security – and if everything goes right they have no idea whether less money could have gotten the same results. This goes right until it goes wrong. When information security goes wrong, the impact could be major.

What is information security? Information security can be defined as “Adequately protecting the confidentiality, integrity and availability of information against possible threat manifestations.” (Verheul, 2011)

Several standards to aid in information security exist. Out of all these standards, ISO 27000 is the most used (Susanto, Almunawar, & Tuan, 2011). ISO 27000 is a range of standards, of which ISO 27001 and 27002 are the most important. ISO 27001 describes a framework to maintain control over information security and ISO 27002 contains a list of controls that could be implemented to mitigate a certain threat. Chapter 2.2 gives more information on ISO 27000.

Inspired by BSIMM, a research project into how software security is used in practice, I have decided to perform a similar quantitative research project by the means of expert interviews. BSIMM gathered data from over fifty computer software companies, and checks what

software security initiatives they have taken. This data is combined into an overview that allows companies to look at their peers: what are they doing and what do they (apparently) think is important? However, the scope of this project is considerably smaller than BSIMM. Some notable differences between the BSIMM project and this research project exist. For more information on BSIMM and the difference, chapter 2.1.

Chapter 4 discusses some practical considerations concerning this research, e.g. selecting a sector – in this case the public sector, selecting interviewees and plans on how to properly execute the interviews.

The data and analysis of these interviews will be discussed in chapter 5.

1.1 *Problem statement*

Many prescriptive approaches to ISO 27002 already exist, e.g. ISO 27003, which is the official standard with guidelines for ISO 27001. Several steps to implement the management framework provided in ISO 27001, called an ISMS, are given. However, descriptive documents, in the way BSIMM describes Software Security, do not exist.

Many organizations don't have the resources or skills to fully perform a risk analysis and to implement an ISMS. Therefore, they might now know which security aspects might be relevant to them. Instead of doing a full risk analysis, an organization could also look at its peers. What do they do? Although following your peers might not be as good as doing an extended risk analysis, it is certainly better than implementing controls without any reason at all.

Modern times call for different approaches to problems. Nowadays, mobile phones and tablets are mainstream. Employees are supposed to work everywhere. Information is quickly shared via social media. How do companies handle these new issues – which controls do they implement and how do they select them?

So far, not a lot of research has been done on the practice use of ISO 27000. This research project can be seen as exploratory: The data gathered in this research could very well be used to formulate hypotheses in other research projects. For more information on existing literature, please read chapter 3

1.2 *Research question*

"What ISO 27002 controls do those in charge of corporate information security choose to implement, and why are these chosen?"

Subquestions

1 "How do those in charge of information security come to a selection of information security controls?
2 "Why are some controls considered to be more important than others?"
3 "What ISO 27002 controls do those in charge of corporate information security consider most important?"

1.3 *Research approach*

The approach taken in this research is qualitative research, by means of expert interviews. Expert interviews are a good way of exploring a research field. The experts often know much about the research topic. By talking to several of them, it is possible to find out if there's a consensus or there's still much debate on certain topics. Both results could be used in further research.

Qualitative research, unlike quantitative research is used to focus more on the 'why' and 'how' questions. Therefore, qualitative research typically takes smaller, but more focused samples than quantitative research. Qualitative research often does not have a clear-cut hypothesis in advance. Instead, it takes an open-ended question. Selection is not done with statistical randomness, but based on what is available. By interviewing those in charge of information security, the aim is to gain insight in what controls they choose and why those were chosen over others.

1.4 *Relevance*

Easier exchange of information is becoming more and more important. For example, within the public sector DigiD will be implemented at all provinces and municipalities during 2013. DigiD is a system that allows citizens to be authenticated online, which can be used for tasks that normally require a citizen to go to their city hall. However, ease of access to possibly private information does not come without risks. DigiD was taken offline at January 9th because of a severe security issue within its underlying framework, Ruby on Rails[1]. According to the NCSC, the Dutch National Cyber Security Centre, this security issue was not abused. This does however underline the need for a thorough process to maintain in control of information security.

As there is very little scientific literature to be found on practice use of ISO 27002, this research can be used as exploratory research. It intends to find out what controls are commonly used and how they are selected. This could be used for future research.

[1] http://www.nu.nl/internet/2999846/digid-offline-lek-in-platform.html

Furthermore, this research could be used by organizations that don't have the resources to do a full risk analysis. They could look to their peers – what controls do they have? What do they think is important when it comes to approaching IS?

1.5 *Outcomes*

The outcomes of the research vary from a very uniform to a widely different response between the different experts. Also, it might be interesting to note what they think is the best approach to information security. What must be in place to ensure that the organization is not missing important aspects to information security?

It is interesting to see how controls are chosen. A lot of organizations don't follow the methodology as described in ISO 27001, but use a much more ad-hoc based approach. In any case, the information gathered during this research could prove very useful for further research.

2 Background

This chapter discusses the background of this research, and what it was inspired by. The biggest inspiration was the BSIMM, a practical software maturity research. The range of ISO 27000 standards was used as a measuring framework for information security.

2.1 *BSIMM- Inspiration*

BSIMM is short for Building Security In Maturity Model. BSIMM4 lists the practice use of the Software Security Framework (SSF) in 111 different companies, including Adobe, Google, Microsoft and others. The SSF is an aggregation of 4 different domains, each containing three practices, e.g. Training and Attack Models.

By quantifying the software security maturity, using SSF, in many different organizations, BSIMM hopes to show what the common ground is, and what differences might exist. The BSIMM is not a "how to" guide, nor is it a one-size-fits-all prescription. Instead, the BSIMM is a reflection of the software security state of the art. (Gary McGraw, 2012)

BSIMM is used as a 'measuring stick'. This means that organizations can compare and contrast their own initiative with what other, similar, organizations do. Using that information, organizations can more easily decide what their next goals ought to be.

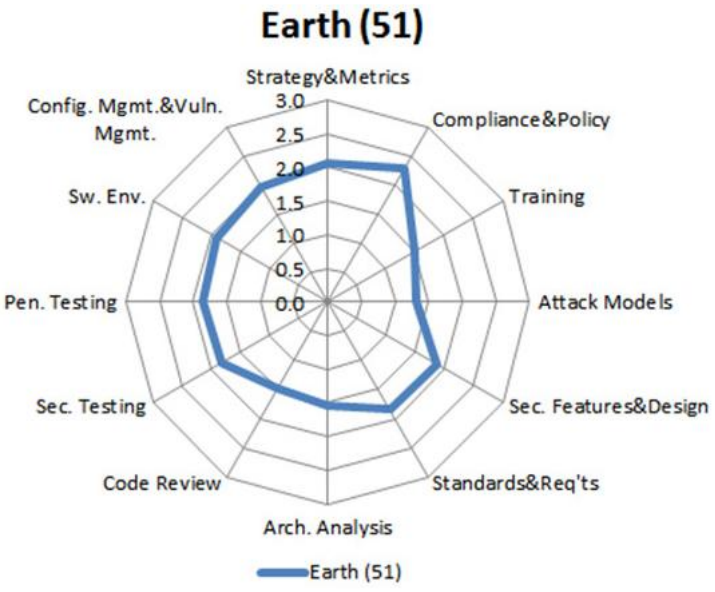


Figure 1: Data of all 51 companies, measured using SSF (Gary McGraw, 2012)

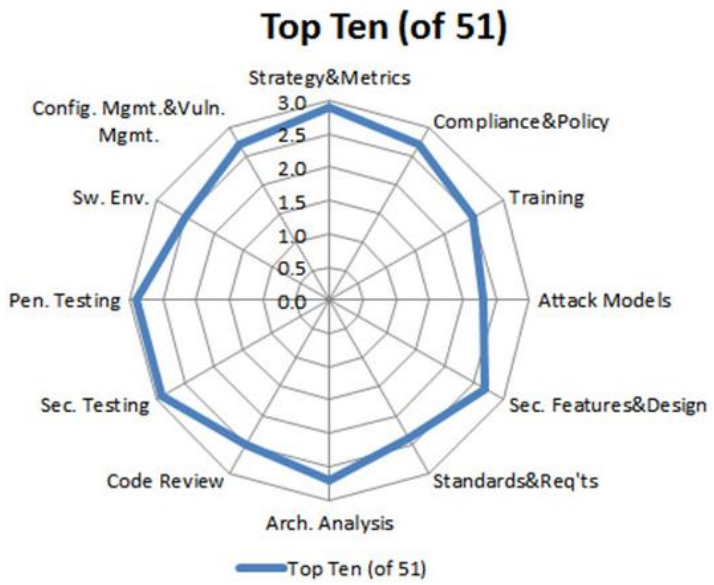


Figure 2: Data of the ten best scoring companies, measured using SSF (Gary McGraw, 2012)

The graphs in figure 1 and 2 show the 12 focal points of the SSF.

Figure 1 shows how the 51 organizations scored on average, and figure 2 shows how the ten best scoring organizations scored on average. One interesting thing to note is that on average, most companies still have to work on training and attack models.

Differences compared to BSIMM

BSIMM was used as inspiration for this research project. There are, however, some big differences between BSIMM and this research.

The biggest difference is that this research has an entirely different focus. BSIMM uses the Software Security Framework[2] to analyze software security, whereas my research covers information security using ISO 27002. Another large difference between this research and BSIMM is that BSIMM focuses on all kinds of software developers, and this research will take a smaller scope of public organizations within the Netherlands. Also, BSIMM analyzed 51 different organizations, whereas this research is much more limited – the amount of organizations will be around ten.

[2] http://www.informit.com/articles/article.aspx?p=1271382

2.2 *ISO 27000*

The ISO 27001 standard was originally called BS 7799, and published by DTI, a part of the UK government. A few years after its introduction, the BS 7799 standard was adopted as the ISO standard for information security. Since then a lot of standards have been added to ISO 27000. The two most important standards in the 27000 range are 27001 and 27002. The first one describing a management framework to take control of the information security within an organization, and the second one being a list of concrete controls that can be implemented to support the information security.

In this research, ISO 27002 is used as a measurement framework for information security within organizations. It's surprisingly well suited for this job, because the idea behind ISO 27002 is to have a list of controls that should be able to mitigate every possible information security risk. The controls can be high-level or very specific. An example of a high-level control is 5.1.1 -Information security policy document. This control describes the need for a document describing the security policy. An example of a specific control is 11.5.5 - Session time-out. This control describes that a session should be shut down after a certain time of inactivity.

The other standards in the ISO 27000 range are support for either 27001 or 27002. They can be guidelines for implementation, guidelines for auditing/certifying or a document that helps implementing ISO 27001 within a specific sector.

Standards in ISO 27000

The ISO 27000 consists of the following:

- ISO/IEC 27000:2009, Information security management systems — Overview and vocabulary
- ISO/IEC 27001:2005, Information security management systems — Requirements
- ISO/IEC 27002:2005, Code of practice for information security management
- ISO/IEC 27003:2010, Information security management system implementation guidance
- ISO/IEC 27004:2009, Information security management — Measurement
- ISO/IEC 27005:2011, Information security risk management
- ISO/IEC 27006:2011, Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007:2011, Guidelines for information security management systems auditing
- ISO/IEC 27008:2011, Guidelines for auditors on information security controls
- ISO/IEC 27010:2012, Information security management for inter-sector and interorganizational communications

- ISO/IEC 27011:2008, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27031:2011, Guidelines for information and communications technology readiness for business continuity
- ISO/IEC 27033-1:2009, Network security -- Part 1: Overview and concepts
- ISO/IEC 27033-3:2010, Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues
- ISO/IEC 27034-1:2011, Application security -- Part 1: Overview and concepts
- ISO/IEC 27035:2011, Information security incident management
- ISO 27799:2008, Health informatics — Information security management in health using ISO/IEC 27002

ISO 27001

ISO 27001 describes an information security management system (ISMS) that makes sure information security is under explicit management control. To do so, a periodical risk analysis should be held, and counter-measures (controls) should be implemented based on that analysis.

ISO 27002

The ISO/IEC 27002:2005 standard, informally called ISO 27002, consists of a list of 133 controls that could be implemented by an organization and a short guide on how to do so for each of these controls. Combined with ISO 27001, these standards are the core of ISO 27000.

The controls are divided amongst the following sections:

- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical Security
- Communications and Ops Management
- Access Control
- Information Systems Acquisition, Development, Maintenance
- Information Security Incident management
- Business Continuity
- Compliance

Other ISO 27000 standards

Apart from the ISO 27001 and 27002 standards, there are ISO several more standards in the 27000 range[3]. These other standards are used as guidance and support for the ISO 27001/27002 for both organizations and auditors.

ISO 27003

ISO 27003 is used as a supporting implementation standard for ISO 27001. This standard goes into getting management approval, defining the ISMS, conducting an organization analysis and doing a risk analysis.

ISO 27004

The ISO 27004 is a standard that aids in measuring the effectiveness of the ISMS.
ISO 27004 consists of the following chapters:

- Information security measurement overview;
- Management responsibilities;
- Measures and measurement development;
- Measurement operation;
- Data analysis and measurement results reporting;
- Information Security Measurement Program evaluation and improvement.

ISO 27005

ISO 27005 is a standard that provides guidelines to implement ISO 27001. The approach that ISO 27005 takes is to first establish the context – defining the scope (primary processes and supporting assets) and boundaries of the organization.

When the scope is defined, a risk analysis will be performed. The risk analysis consists of identifying assets and the threats they face. Furthermore, the impact of a successful exploitation of a certain threat must be analyzed. When these are done, for each threat an estimate of chance that the threat will successfully be exploited will be multiplied by the costs of the impact of that exploit. Given that list, each risk should be either mitigated by implementing controls, accepting the risk, avoiding the risk or transferring the risk.

ISO 27006 and certification

An organization can be ISO 27001 certified. This can only be done by accredited auditors. The organization can only be certified if the ISMS and a number of controls are properly implemented. The ISO 27002 standard defines the way in which an auditor can assess an organization in order to accredit it. ISO 27002 defines two stages to accredit an organization.

[3] http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO_IEC_27000_2009.zip

The first step is a documentation audit, in which the auditor will conduct interviews and research the existing documentation. The second stage consists of checking for proper implementation of the controls, as mentioned in the documentation. If an organization gets certified, the certificate will only be valid for a predefined time span, typically three years. During these three years, a yearly check-up – the Surveillance Audit is required. After these three years, the entire certification process will have to be done again.

2.3 *COBIT*

Control Objectives for Information and Related Technology, or COBIT, is a framework for IT management and IT governance.

The first version of COBIT was released in 1995; the current version is version 5 and was released in 2012. COBIT defines some generic processes to manage IT. Each process is defined with process inputs and outputs, process objectives and a basic maturity model.

COBIT contains the following components:

- Framework: Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements.
- Process descriptions: A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.
- Control objectives: Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.
- Management guidelines: Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.
- Maturity models: Assess maturity and capability per process and helps to address gaps.

3 Existing research

This chapter will describe literature that is relevant to the research. There was no literature on practical research using ISO 27000 to be found, using Google Scholar and Web of Science. Almost all results had a very limited number of references (<5). However, some still were of use. The following paragraphs describe what literature was used for the research.

There are very few scientific papers on the ISO 27002 standard, and none were found that research practice use of ISO 27002 controls.

Gerber & Solms (2008) show which ISO 27002 controls are related to Intellectual Property Rights, Legislation, Contractual Obligations and International Laws. These tables might be useful when deciding which controls should be the focus of these interviews, or should be disregarded as a whole. (Gerber & Solms, 2008)

	CONTRACTUAL OBLIGATIONS									
	External Agreements & Third Party Arrangements	Confidentiality Agreements	Outsourcing	Service Level Agreements	Licensing Agreements	Quality of Code	LABOUR LAW		Trading / information Service	SW escrow (elec./ manual exchange)
							Employee Condition of access statements	Contract of Employment		
6.1.5		X								
6.1.6										
6.2.2										
7.1.3	X							X		
8.1.3	X	X						X		
10.8.1	X	X						X		
11.7.2		X			X					
12.5.5	X		X			X				X
15.1.5	X						X	X		
15.1.6		X								
...										

Figure 3: Example of a table shown in the paper (Gerber & Solms, 2008)

Von Solms & von Solms describe ten big, often made mistakes. E.g.:

- "Sin number 9: not realizing the core importance of information security awareness amongst users" (von Solms & von Solms, 2004)

This information is useful when selecting which controls to talk about in the interviews. As these ten are commonly made, these will have to be included in the list of ISO controls. A full list of these ten sins and what they are used for can be found in chapter 4.3. To make sure the interviews will be conducted in a scientifically sound method, some scientific papers on interviews/qualitative research are used.

Polkinghorne (2005) describes data collection in qualitative research, focusing on participant interviews. He makes plenty of useful statements for qualitative research, like:

- “The data serve as a ground on which the findings are based. In constructing the research report, the researcher draws excerpts from the data to illustrate the findings and to show the reader how the findings were derived the evidential data.” (Polkinghorne, 2005)
- “It is not the printed words themselves that can be analyzed by counting how many times a particular word appears in the text. Rather, the evidence is the ideas and thoughts that have been expressed by the participants.” (Polkinghorne, 2005)
- “Participants and documents for a qualitative study are not selected because they fulfill the representative requirements of statistical inference but because they can provide substantial contributions to filling out the structure and character of the experience under investigation.” (Polkinghorne, 2005)

4 Research methodology

In this chapter, the methods of selecting a sector to research and what organizations to approach within that sector are discussed. Furthermore, a first step towards an interview plan is described.

4.1 *Sector*

For this research, experts within the public sector are interviewed. These experts hold the title of security officer, or whatever comes closest in their organization. There are two big reasons for choosing this sector:

The first reason for choosing the public sector is that there are some interesting problems specific for that sector. For example, government organizations usually have a lot of privacy sensitive data – e.g. citizen information. Within the Netherlands, a database of citizen data exists. This database is called the GBA. Furthermore, it seems that data leaks from public organizations are often well exposed in the media[4].

The second reason for choosing organizations in the public sector is availability. Ernst&Young has a lot of clients within the public sector. With the goal of performing around ten interviews, and a worst-case guesstimate of 1/3 of the organizations willing to cooperate, a sector with at least 30 possible organizations was needed.

4.2 *Approaching organizations*

Out of the client database of Ernst&Young, a number of possible interviewees were selected. The method to selecting them was mostly a matter of availability. Out of the client database a shortlist was created, and a letter was sent to each of the possible interviewees on that list.

In discussions with experts at Ernst&Young, it was decided that the duration of the interviews would be one hour. They argued that asking for more time would lower the amount of cooperating organizations too much.

The letter contained information on what the research content was, what would be asked of them and what their own benefits were. Some organizations took initiative and replied themselves, others required a phone call. In total, 5 out of 18 organizations agreed to participate. This corresponds with 28%.

[4] http://www.nu.nl/internet/2885141/hoge-kosten-dorifelvirus.html
http://www.nu.nl/algemeen/666632/geheime-informatie-defensie-weer-op-straat.html

4.3 *Controls and topics*

The list of controls in ISO 27002 consists of 133 elements. As these are far too many to all cover within a one hour interview, some of them will be grouped with others and some will not be used at all. To select the controls, two different types of sources were used. The first being literature on information security. Looking at dos and don'ts, these were mapped to controls in ISO 27002.The other type of source was expert input at Ernst&Young. They have experience in auditing based on ISO 27002, as well as interviewing information security in general.

Ten deadly sins

Von Solms & von Solms created a list of 10 deadly sins, which should be avoided at all costs. The list consists of the following items:

1. Not realizing that information security is a corporate governance responsibility (the buck stops right at the top)
2. Not realizing that information security is a business issue and not a technical issue
3. Not realizing the fact that information security governance is a multi-dimensional discipline (information security governance is a complex issue, and there is no silver bullet or single 'off the shelf' solution)
4. Not realizing that an information security plan must be based on identified risks
5. Not realizing (and leveraging) the important role of international best practices for information security management
6. Not realizing that a corporate information security policy is absolutely essential
7. Not realizing that information security compliance enforcement and monitoring is absolutely essential
8. Not realizing that a proper information security governance structure (organization) is absolutely essential
9. Not realizing the core importance of information security awareness amongst users
10. Not empowering information security managers with the infrastructure, tools and supporting mechanisms to properly perform their responsibilities

These ten sins focus on the fact that information security is a business / management / corporate governance issue, and not purely a technical one. Therefore, controls that focus on processes that maintain control over information security will be included.

Also, point 4 argues that there should be a risk analysis. This will be included in the interview.

Finally, point 9 says that awareness amongst employees is key to information security. The corresponding ISO controls will be included.

Expert input

By talking to experts at Ernst&Young, a list of controls to be used in the interviews was conceived, where each control would be colored either green for ‘must include’, yellow for ‘might include’ and red for ‘do not include’. For the list of controls, see Annex A. The focus of the controls, according to the experts at Ernst&Young, should be on how businesses stay in control of their information security. E.g. information security policy, continuity and incident management, etc.

A couple of examples of red controls are:

#	Name	Description	Reason for red color
8.2.3	Disciplinary process	There should be a formal disciplinary process for employees who have committed a security breach.	Not too important for the organizations in the public sector, as willful employee security breaches can be handled case by case.
9.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.	Too specific to include in an interview.
10.10.6	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.	Too specific.
12.2.1	Input data validation	Data input to applications should be validated to ensure that this data is correct and appropriate.	Too technical.
12.4.3	Access control to program source code	Access to program source code should be restricted.	Obvious and too technical.

The yellow controls were seen as more relevant than the red controls. However, as the time was severely limited these controls were not included in the interview schema. If the topic came up during the interview, it was followed up on. If the amount of time for each interview was higher, the yellow controls would be included first. These are a couple of examples of yellow controls:

#	Name	Description	Reason for yellow color
8.1.2	Screening	Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.	Completely going through their background verification check would take too long.
10.4.1.	Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.	It seemed that every organization would say that they have virus scans. This does not mean that this control is not important for organizations.
10.6.2	Security of network services	Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided inhouse or outsourced.	Too technical.
12.3.2	Key management	Key management should be in place to support the organization's use of cryptographic techniques.	Too specific/technical.
12.5.4	Information leakage	Opportunities for information leakage should be prevented.	Too vague; it would take too long to fully cover this topic.

Apart from a list of important controls, the expert input also provided some interview approaches for each control, which are also included in Annex A, in Dutch.

Grouping the controls

The green controls were taken and put into categories. These categories are then used as topics for the interviews. The topics are as follows:

- Policies
- Employees
- Third parties
- Information storage/access including hiring / letting go of employees

- Physical security
- Software development and change management
- Ex post analyses
- Incidents and continuity

For each of these topics some subtopics were made. These subtopics reflect all the controls in a certain topic.

4.4 *Interview plans*

Opening statement

A word-for-word opening statement seemed a bit excessive. However, it still was deemed important to cover a few bases before starting with the actual interview. Therefore, the following instructions were noted in the interview plan:

1. Short introduction the background of the interviewer, background of the research project
2. Contents of the interview
    a. Going through the list of predefined questions / controls
    b. Talking about which controls are more important than others
3. Duration of the interview
4. Anonymity
5. Recording of the interview / making notes
6. Write-up / correspondence about the write-up

Questionnaire

After the introduction, the interview consists of two parts. The first part is doing a quick scan through the controls they use by more or less predefined questions or topics. There are eleven subjects, with each multiple questions to cover.

With expert input of the professionals at Ernst&Young, the questionnaire was made based on the list of controls in Annex A. Only the green controls – the 'must include' controls were selected for the questionnaire, as the time for each interview is very limited.

Based on the previously conceived subtopics, questions were made. These questions were directly used in the questionnaire. The questionnaire is in Dutch, because all the interviews would be held in Dutch as well. Table 1 shows the list of questions used in each of the interviews. For a full interview sheet, please refer to Annex B.

Topic	Question / subtopic
Beleid	Is er informatiebeveiligingsbeleidsdocument? Zijn de verantwoordelijken belegd bij de juiste personen? Is er draagvlak van het informatiebeleid door het management – ondertekend? Is er een security officer aangesteld – zo ja, heeft hij andere taken?
	Ligt er een risico-analyse ten grondslag aan het beveiligingsbeleid? Beschikbaarheid Integriteit Vertrouwelijkheid Risico Kans Maatregel
	Zijn er nationale richtlijnen vanuit de overheid?
	Wordt het beleid en de uitvoering daarvan onafhankelijk getoetst aan de hand van ISO 27001?
Personeel	Zijn er geheimhoudingsverklaringen? Zo ja, op basis waarvan?
	Zijn er security awareness trainingen? Zo ja, wat voor trainingen, hoe vaak, etc?
Externe partijen	Wordt er gebruik gemaakt van externe diensten, zoals schoonmakersbedrijven/servers op andere locaties/externe beheerders? Zo ja, hoe wordt de veiligheid gewaarborgd?
	Zijn er contractueel regelingen vastgelegd?
	Hoe wordt er omgegaan met vertrouwelijke gegevens als die opgevraagd worden door de burger? Identificatie etc.
	Is er een plan over hoe informatie uitgewisseld wordt met andere gemeentes, overheid, ?
Informatieopslag/ en logische toegangsbeveiliging bij	Is er een inventaris van welke informatiebronnen welke informatie bevatten? Is er een eigenaar voor iedere informatiebron? Fysieke locatie, bij digitale bron: op welke server, wie mag toegang hebben?
	Hoe worden oude datadragers vernietigd? Oude pcs? Papier?
	Worden er backups gemaakt en getest?
Indienst/uitdienst/ functiewijzigingen	Hoe wordt er rekening gehouden met publieke informatie – websites, digid?
	Zijn de netwerken fysiek of digitaal gescheiden ingeregeld? Bijvoorbeeld, zitten baliemedewerkers op hetzelfde netwerk als de servers?

	Zijn er complexiteitseisen voor wachtwoorden? Is er aan de hand van een risicoanalyse bepaald hoe complex deze wachtwoorden moeten zijn?
	Is er een beleid voor hoe medewerkers hun computers behoren te behandelen en wordt hierop gecontroleerd?
	Is er ingeregeld wie welke informatie mag meenemen – fysiek uit archief? Hoe wordt er gecontroleerd dat dit juist gebeurt?
	Zijn er vaste procedures bij indienst met specifiek bepaling van welke toegangsrechten zij behoren te hebben /uitdienst inclusief inleveren van middelen en opheffen rechten? /functiewijzingen incl aanpassingen van rechten?
	Mogen medewerkers informatie meenemen? Denk aan USB-sticks, computers, fysiek uit archief? Wordt hierop gecontroleerd?
Fysieke beveiliging	Hoe is de fysieke toegang geregeld?
	Hoe zit het met deels openbare locaties? Gemeentehuizen ed?
	Is thuiswerken mogelijk? Zo ja, hoe wordt er gezorgd dat alleen medewerkers daar gebruik van maken? Zijn alle informatiebronnen te benaderen vanaf thuis?
	Is het mogelijk om mobiele devices die in beheer van de medewerker zijn mee te nemen (smartphones, tablets)? Zo ja, hoe wordt dit veiligheidsrisico afgedekt?
Software-ontwikkeling en change management	Is er een procedure omtrent het beheer van wijzingen? Als er nieuwe systemen ontwikkeld worden, is er een procedure om vast te leggen wat er precies ontwikkeld wordt – requirements, functioneel ontwerp, technisch ontwerp, etc.
	Aparte ontwikkel/test/productieomgeving? – evt acceptatieomgeving
	Penetration testing of andere praktijktesten?
Ex post-analyses	Wordt er gelogd?: voor Veranderingen van data buiten de applicaties – bijv door systeembeheerders direct op de database? Fouten en andere onverwachte gedragingen van system Wordt er standaard de logging gecontroleerd (proactief) of alleen wanneer er iets mis gaat(reactief)?
	Wordt er gecontroleerd of de logs niet handmatig zijn aangepast?
	Wordt er audit-informatie bijgehouden?
Incidenten en continuiteit	Is er een incidenten-meldpunt? Waar is die ondergebracht? Hoe worden incidenten gedocumenteerd?
	Kunnen daar ook zwakheden in fysieke of digitale beveiliging gemeld worden?

	Is er bepaald wat het management moet doen om een incident af te handelen?
	Wordt de impact van een incident naderhand bepaald, om te kijken of er geen onvoorziene gevolgen zijn opgetreden?
	Is er bepaald welke processen bedrijfskritisch zijn en welke systemen daarvoor gesteund wordt?
Legislatie en standaarden	Is er in kaart gebracht welke wetten van belang zijn? Zo ja, welke wetten? Bijv wet openbaar bestuur, wet bescherming persoonsgegevensp
	Worden er bepaalde standaarden nageleefd? ISO 27001?

Table 1: Interview questions

Each of these topics is to be discussed, and based on this discussion the topic would be

- Colored green for 'in order'
- Colored yellow for 'some things are in place, but lacking'
- Colored red for 'Absent'

This color-coding should be done in consultation with the interviewee.

Unstructured part of the interview

After the questionnaire, a more freeform interview takes place. In this part of the interview, the interviewer asks the interviewee about what he, as a representative of his organization reckons is important when it comes to approaching information security.
This part of the interview has no set goal and/or results.

Closing statement

Just like the opening statement, there was no exact statement. However, the following points should be handled:

1. Thanking them
2. Follow-up of the write-up
3. Explanation of what the final product will be

4.5 Follow-up

After each interview, an interview report is written. In this report, the gist of the interview should be conveyed. Each interview report will be sent to the interviewee, allowing him to correct any mistakes made in the report. This way, the validity of the reports is guaranteed.

The same approach is taken for the color coded questionnaire. If the interviewee feels that his organization should score higher or lower on a certain topic, with sufficient argumentation, the score can be changed.

5 Data and analysis

This chapter describes the data gathering and analysis thereof, after the interviews were held.

For each interview, a report was made. The size was limited to circa one page. The following section contains the reports for each interview. For anonymity reasons, the organizations are numbered with roman numerals. The reports for each organization can be found in chapter 5.1. The results from the questionnaire for each organization can be found in chapter 5.2. There, for each organization the scores for each subtopic are shown. In this chapter, the data from the first two chapters are combined into an analysis.

One important thing to note is that the data of these interviews is limited to what the interviewees tell me. This means that the existence of controls mentioned during the interviews was not checked. Therefore, it is not known if the design is being properly followed, how effective it is etc. Another downside is that various psychological effects come into play. For example, a security officer might be ashamed of what he might consider personal failure, and make the situation seem better than it actually is. However, in my experience many interviewees did not try to mask any problems within their organizations. Often, they would tell stories of how they could get in without authorization – because they knew the situation very well. Others explained that they knew what situations needed improvement – yet the management was not committed enough to information security to improve the situation.

For each interview, a report was made. The size was limited to approximately one page. The following section contains the reports for each interview. For anonymity reasons, the organizations are numbered with roman numerals.

The interviews took one hour or slightly more. Although for only one hour was asked, often the interviewees seemed to enjoy the discussion about developments within their working area, allowing the interview to take some more time than was actually planned.

5.1 *Interview reports*

For each organization, three provinces and three local councils, a report of approximately one page was made. Any opinions in these reports are the opinion of the interviewee, unless stated otherwise. The reports were made in consultation with the interviewees, and therefore reflect their opinions.

Organization I

The interview was held with one of those responsible for information security within this organization. The organization has roughly 500 employees.

Situation in the organization

Within this organization, there is no specific security officer. However, a group of people is responsible for information security. The information security policy was created in 2009, and is signed off by the management. However, the IT security policy is not signed off by the management.

The organization intends to place as many systems as possible with third parties. Whenever this is done, a clause on information security is included within the contract.

Every now and then – approximately yearly, 'awareness days' are held for the employees. The main goal of these days is to make employees aware of the fact that they are not proficient when it comes to assessing security issues.

There is a lack of control of information sources and processes. There is a process for WOB[5] requests. For change management, a clearly defined process exists. However, the changes are usually done by a third party.

It's possible to work at home. However, not every system can be accessed when working from home for security reasons.

Important controls

For this organization, the most important controls are those that concern governing information security, e.g. high-level policies, assessing risks. This means that the following three documents must exist and be signed by the management:

- Information security policy
- IT Policy
- Classification of information sources

Also, security awareness should be emphasized. Within this organization, awareness training is held to make employees knowingly inept in information security, instead of unknowingly inept.

[5] Wet Openbaarheid van Bestuur, a Dutch law stating that any government organizations must provide any government-held information when it is requested.

He feels that a specific security officer is required, and should be accredited by management. At the moment, there is not a single point of responsibility for security issues.

The management should become more aware of security issues themselves, to play an exemplary role towards other employees. An example of this is: According to the information security policy, ID badges need to be shown at all times. The management does not do this themselves.

One of the major future changes to the work environment is that everything should be accessible all the time everywhere. At the moment, only documents and e-mail are accessible from other locations. More improvements to identity management are needed to make sure the risks are minimized.

Organization II

The interview was held with the security officer, which in this organization is a part of the IT department. The organization has roughly 750 employees.

Situation within the organization

One of the major issues within the organization is that information security is not an integral part of the organization, but something that is considered a problem for IT. This results in several issues for the security officer, for example:

- Lack of management commitment – the information security policy has not been approved / signed by the management.
- Not all information security issues are technical ones. For example, in the past employees did not require a non-disclosure agreement. This has been changed in spring 2012, requiring that all new personnel sign a non-disclosure agreement.
- There is no confidentiality classification for information.
- There is no listing of processes within the organization.

There are several courses for employees, e.g. a LinkedIn course or an Office course. However, there is little to no attention to information security within these courses. The employees have little knowledge of how their (online) actions could harm the image of the organization.

The third party contracts all have clauses regarding information security. This includes the cleaners. An external company disposes of paper and used hard disks.

There are procedures for employment, both new employees and termination. However, these procedures are not always properly followed – employees only get more access rights and hardly ever fewer, even if their job no longer requires it.

The property is physically protected with access cards. There are different zones, e.g. public zones, semi-public zones, employee only zones and protected zones.

The wireless network is also segregated for different uses. Smartphones and tablets are allowed, but only on the intended wireless network.

Each year, two penetration tests are performed. For example, by leaving USB sticks around and checking how the employees react.

It's possible for employees to work at home. The authentication works with a SMS-token, which will grant the user similar access to what's possible when physically at the office.

Approach to information security
According to the security officer, these steps are needed for a proper approach for information security:

1. Information security should be integral in the organization.
2. Awareness of information security risks amongst the employees
3. The IT will automatically follow if the first two points are in order

There should be a proper inventory of information and processes. Also: even within the public sector, organizations should pay attention to business cases – including the business case for certain information security controls.

Organization III

The interview was held with the security officer. This organization has about 650 employees.

Situation within the organization
The organization has recently undergone a merger, which has led to a recent start-up to create processes for information security.

As of now, there is no information security policy yet. However, interviews have been held with experts within the organization to create a list of ISO 27002 controls that ought to be implemented.

The systems that are used are shared with other organizations, in a shared service center. That center also includes a service desk for incidents. For high priority incidents, a process is in place that includes the management and an impact analysis.

It's possible to work from home. However, the GBA is only accessible from the office, where only authorized employees have access. The national government periodically takes samples from the log of accessed citizen files, and asks for an explanation.

Physical access is regulated with the use of tokens, where access is distributed on a need-to-have basis. The desks for public services have emergency buttons, which can be used if a disturbance occurs within the freely accessible areas. At night, the inner courtyard is locked off with fences by the security team.

The organization has had penetration tests, e.g. by using a mystery guest. A mystery guest is someone hired by the organization to impersonate an outsider who is trying to gain access to critical information. This mystery guest made a video of how to enter. This video was shown to the management, to create awareness amongst them.

It's possible to bring a mobile phone or tablet computer. There are three different wireless networks – a public one, one for guests and one for employees. These use a ticket system, which only allows a device for a certain amount of time. Afterwards, a new ticket must be requested.

Old computers and paper are disposed of by a third party.

Approach to information security

As this organization has recently undergone a merger, the approach that the security officer would take in general is the same as he recently took.

The following steps should be done, according to the security officer:

1. Risk analysis
2. Starting document
3. Prioritizing
4. Creating a policy

Organization IV

The interview was held with the security officer. The organization roughly has 4500 employees.

Situation within the organization

Within this organization, ISO 27002 is used as a guideline for information security. Currently, a baseline is being applied throughout the entire organization.

At the moment, a classification for information is under development. This classification can then in turn be used for the baseline.

On third parties: Old papers are disposed of by a specialized company. In the future, it will also be possible to dispose of other types of media (CD's, DVD's, flash media) in a similar fashion. For as much software as possible, a SaaS solution is used. However, change management is still done within the organization.

Backups are made regularly and tested as well.

Physical security has three different zones: Public areas, employee areas and specific areas, for example server rooms. The public areas are strongly monitored.

Approach to information security

According to the interviewee, the following approach should be taken:

1. Making sure the right people take their responsibilities. This includes that management should be explicitly committed to information security.
2. A security officer should be assigned.
3. The security officer should analyze risks and come up with possible solutions. These possible solutions should be presented to management – including projected benefits and costs of a certain solution. The management decides whether certain costs are worth the benefit.
4. Focus on incident and continuity management to make sure if something is wrong, it will improve. An ISMS should be made to get and stay in control.

Organization V

The interview was held with the security officer in the organization, who is part of the IT department. The organization has about 1500 employees.

Situation in the organization

In this organization, a difference is made between the information security policy and the information security plan. The policy is more high level than the plan. The plan is based on ISO 27002 controls. The controls are chosen using a risk analysis: A matrix of estimated

risks and impact is made and used as a basis for selecting controls. For practical support to implement these controls, PvIB[6] guidelines are used.

The employees of this organization have sworn an oath of office, except for temporary personnel. They have to sign a non-disclosure agreement instead. Employees are advised on information security by using intranet bulletins, but there is no policy in place for security awareness training.

For third parties, for example the hosting of applications, clauses on information security are either included in the terms of service or included in the contract. More and more cloud based applications are used. According to the security officer, these are harder to get a grip on. A third party takes care of any hardware that needs disposal, including paper, old computers, printers, etc.

When it comes to new applications, off-the-shelf solutions are preferred to custom software. If need be, they can be altered to support additional requirements. For large applications, a public tender procedure is held. There is a formal procedure for change management, which has improved greatly over the past few years.

For inter-government communication, a closed government network called Gemnet is used.

There is no organization wide listing of what server/application contains what information. However, each application has an owner, and the owner is supposed to keep a listing of what information the application requires and holds. Some time ago, an inventory of personal information was made to comply with the WBP[7].

There are several networks within this organization, and they are separated either physically or virtually. For example, there's a network that employees are on, one for the servers, a public wireless network, a wireless network for employees. The latter two can be used for mobile devices, and are therefore not connected to other networks.

Weekly, a list of terminated employees is generated and used to make sure these employees no longer have access to applications. There is a procedure for employee transfers. However, because a transfer can take some time in which the employee might still need his old access rights, this is harder than hiring and termination.

[6] Platform voor InformatieBeveiliging, or platform for information security
[7] Wet Bescherming Persoonsgegevens, a Dutch law protecting personal information

It's possible to work from home. A virtual desktop system is used, giving a virtual workplace at home. In the future, the computers at the office will be using the same system. In the office, all office space is flexible: no fixed rooms for employees.

For incidents, a form exists on the intranet. Depending on the incident, it is assigned to either facility management or the IT department. There it is given a priority, based on the impact of the incident. An escalation procedure exists: the bigger an incident is, the more the amount of follow-up an incident gets. This could include management or an evaluation afterwards.

Approach to information security
The approach to information security within this organization is based on a yearly cycle in which the information security plans are revisited. Every year, an analysis is done of the current situation, including taking a random of sample for certain controls to see if they worked in proper order. Things that are also discussed at this time are things like access cards, making sure the organization is still compliant with laws and guidelines, etc.

A controller from each department is included in this yearly cycle, partly to provide the necessary management commitment.

The approach is comparable to the Plan-Do-Check-Act cycle/Deming cycle, as defined in ISO 27001.

5.2 *Questionnaire data*

The following data was taken from the questionnaires. The questionnaire can be found in Annex B. For each subtopic on the list, the organization was graded green, yellow or red. Green for in proper order, yellow for 'implementation exists but lacking' and red for not in order. To make this information more digestible, the color coding was changed to numerical values. Red is equal to one, yellow is equal to two and green is equal to three points.

For each subtopic, the interviewer and interviewee discussed what the grade should be. The interviewee was included in this, because his opinion would color the scores anyhow. Green was given when the interviewee thought it was all in order, and red if the control was not used or seriously lacking. A typical statement that would lead to a yellow score would be "We have an implementation for that control, but…" Usually the interviewee had a good idea of what the status of their control was.

The following table shows an overview of how the five organizations scored on each of the subtopics. For information on the questions for each subtopic, please read Annex B.

Topic	Subtopic. Organization	I	II	III	IV	V
Policy	1. Information security policy	3	2	1	3	3
	2. National guidelines	3	3	3	3	3
	3. Based on ISO 27001	3	3	3	3	3
Employees	4. NDA	3	2	3	3	3
	5. Security awareness training	1	1	1	2	1
Third parties	6. General third parties	3	3	2	3	3
	7. Contractual clauses	3	3	1	1	3
	8. Information sharing	2	2	3	2	3
Logical access and functional changes	9. Inventory of information sources	1	3	3	2	3
	10. Destruction of old media	3	3	3	3	3
	11. Backups	3	3	3	3	3
	12. Public information	3	3	3	2	3
	13. Network segregation	1	3	3	1	3
	14. Password complexity	3	3	3	3	3
	15. Clean desk policy	2	3	3	2	2
	16. Information access	1	1	3	3	2
	17. Functional changes	3	2	2	2	3
	18. Taking information home	1	1	1	1	2
Physical security	19. General physsical security	3	3	3	3	2
	20. Public areas	3	3	3	3	2
	21. Working at home	3	3	3	3	3
	22. Bring your own device	3	3	3	3	3
Change management	23. Change management	3	3	3	3	3
	24. OTAP	3	3	3	2	3
	25. Penetration testing	2	3	3	3	2
Ex post analysis	26. Logging	2	2	3	2	3
	27. Tamperproof logging	1	1	3	1	1
Incidents and continuity	28. Incident	3	3	3	3	3
	29. Weaknesses in security	3	3	3	3	3
	30. Management role in incident management	3	3	3	3	3
	31. Analysis after security incident	2	3	3	3	3
	32. Business continuity management	1	3	3	3	3
	33. Redundancy	2	3	3	3	3
	34. Keeping plans up to date	1	2	3	3	3
Legislation	35. Laws	2	3	3	3	3
	36. ISO 27001	3	3	3	3	3

Table 1: Organization scores on subtopics

5.3 *Comparison of organizations*

Using the interview reports and the questionnaire data, an analysis was performed.

Please note: the fact that numbers are used does not mean that they can be used for statistical analyses. The sample size is too low to find any correlations and causations. Furthermore, the method of gathering these numbers is still very subjective – they are the result of an opinion of an employee of an organization and are interpreted by a subjective researcher.

However, by using numerical values it's easier to compare the organizations. If a certain topic has a lot of deviation of similar values, it might warrant more investigation. This investigation can be done by looking over the interview reports – do they have anything to say about these topics?

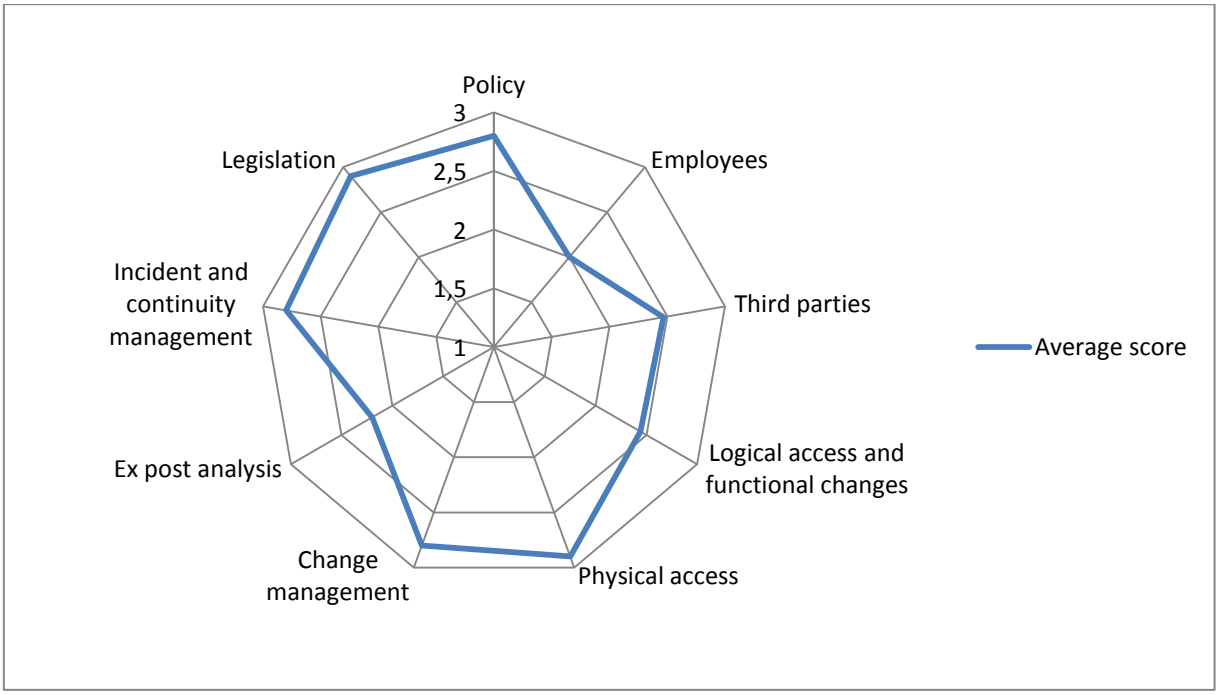


Figure 4: Average scores per topic

The spider chart above shows the average scores of the interviewed organizations, each on a scale from 1-3 where 1 means no controls were implemented and 3 means that all controls were implemented and in proper order according to the interviewees. The three topics that scored the lowest on average are given an extra look.

Employees

The topic with the lowest average score is 'Employees'. Looking at the interviews, this makes sense. Most interviewees agreed that their employee information security awareness programs need a lot of improvement.

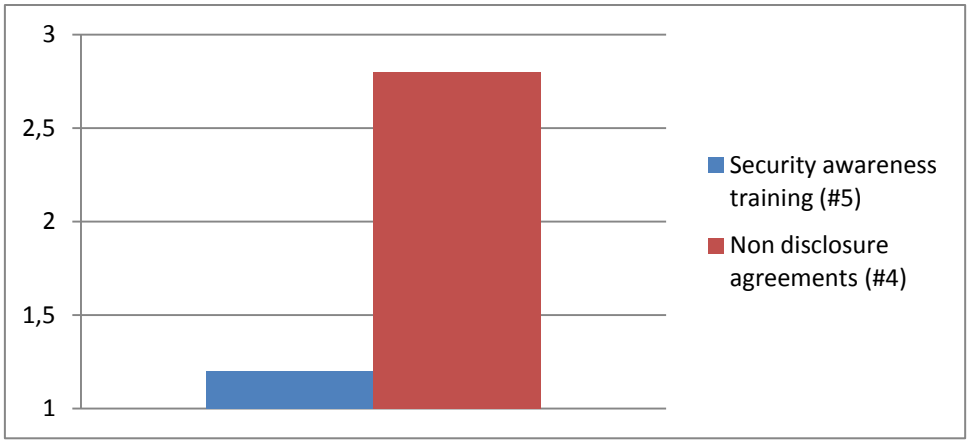
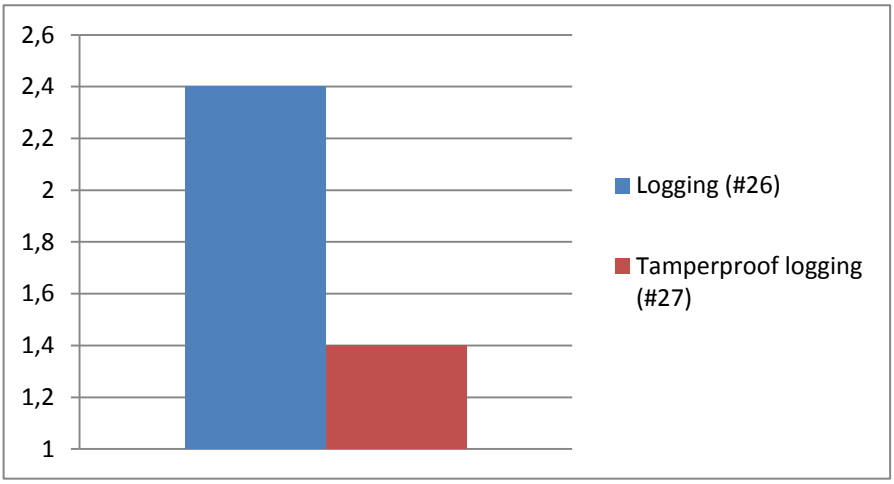


Table 2: Average scores of 'employees' topic

The table above shows the average scores of the subtopics on employees. As can be seen in the graph, the average for security awareness training is only 1.2 – meaning that only one of the organizations scored higher than 1 on this subtopic. For this subtopic, the interviewees were asked what kind of security training the employees had, how often these had, what they focus on. Most interviewees admitted this was lacking, but also that it could be hard to get the organization and employees to see the importance of these trainings.

Ex post analysis

Another low scoring topic is ex post analysis. Logging is not always enabled, for performance reasons. When logging is enabled, the log files are usually only reviewed if something went wrong. Only one organization pro-actively checked the log files for discrepancies.



Tabel 3: Average scores of ex post analysis

However, none of the organizations were able to guarantee that the log files were not tampered with – some of them explicitly said that a good hacker would probably be able to cover his tracks.

Logical access

The third lowest scoring topic is logical access control and functional changes. Within this topic, the lowest scoring subtopic is subtopic 18. That subtopic concerns whether there is a protocol for what information employees can take, for example by using USB sticks, CDs, DVD's, etc.

The interviewees argued that this control had too many downsides for them to implement it: it would require strong regulation of what goes in and out of the building – so much that it would cost too much to implement, and would obstruct employees too much in their day to day activities.

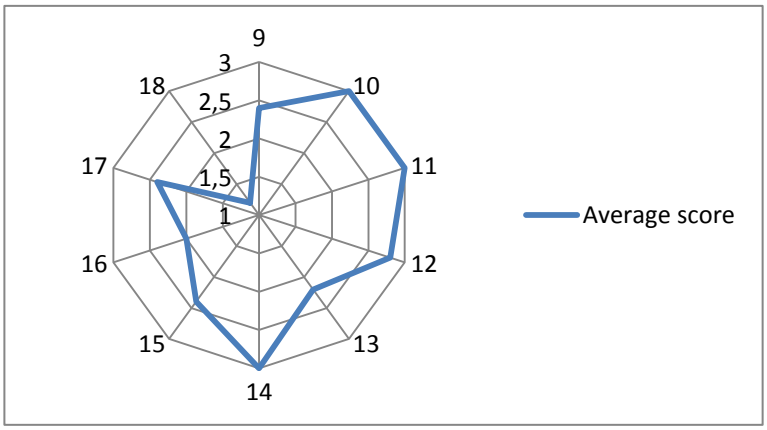


Figure 5: Average scores of subtopics within logical access and function changes

Incident and continuity management

In my own opinion, incident and continuity management seemed to be covered well by the organizations. Plans were made for a big range of possible incidents, e.g. fire in physical locations, power outage or issues with server hardware. Based on the type of possible incident, redundant hardware would be used, or a physical fallback location. All of the organizations also had one or more physical locations in which citizens could still be serviced. This makes sense, as the organizations are required by law to processes certain requests within a certain amount of time.

Third parties

The subtopic with the biggest differences was the one that concerns third party contracts, e.g. whether contracts with hosting companies, cleaning companies, etc. have clauses on protecting information. The interviews support the data: The organizations that pay attention to information security in their contracts also make sure all contracts have proper clauses, whereas other organizations have not paid attention to information security clauses at all.

Other topics

The other three topics, policy, legislation, and physical security, all had (almost) every control implemented. However, this does not mean that there are never issues with these topics. It means that on an organizational level, they cover their bases. Most of the interviewees said that despite their best efforts, it was usually possible to get in the employee area. For example, people holding doors for others was an issue that was hard to improve upon, but could compromise physical security.

Every company had a security policy, and legislation was usually covered well, as organizations in the public sector have had a lot of laws to adhere to, long before the advent of the modern computer society.

Personal impression

Personally, I found that the interviewees took information security very seriously, and usually did whatever was in their power to improve the situation. Some of them were obviously frustrated by the fact that information security was not seen as important enough in their organization. Often the responsibility for information security lied solely with the IT department, not giving the security officer enough room to take care of other issues – issues that could for example be of a contractual nature or something that requires higher management.

Also, communication between the organizations was taken very seriously. In the case of the provinces, every few months the security officers of the provinces gather to discuss new issues. E.g. the DigiD implementation of 2013. This discussion platform is called CIBO or Centraal InformatieBeveilingsOverleg. The fact that the national government is taking information security more seriously is also supported by them launching the National Cyber Security Centre in January 2012[8].

5.4 *New problems*

During the interviews, some new, contemporary issues were also discussed. Two different issues were named by all the interviewees. In their opinion, these new issues were hard because not only the organization needs to adapt, the employees and their culture need to change as well.

1. A major challenge for them is allowing employees to **work at home**. On one hand, it could boost productivity and morale, but on the other hand it could introduce a number of security issues.

   Arguably the biggest problem is that physical security is no longer an option if you want to allow employees to do everything from home. Also, legislation can be an issue. For example, by law the GBA can only be accessed from a physical location that belongs to the government. This raises an important question: Which is more important, allowing government employees to work at home, or risking possibly privacy sensitive data? The interviewees generally want to take advantage of modern technologies. However, they also feel that to allow employees to work at home, you need to be able to trust them and their competence in assessing information security risks. This is why most interviewees have opted to allow people to work at home, but not to give them access to more critical systems when they do so. E-mail and their current documents can generally be accessed.

[8] http://www.rijksoverheid.nl/nieuws/2012/01/12/nationaal-cyber-security-centrum-geopend.html

2. Another challenge is **social media**. According to some interviewees, in the past people would only be a government official during working hours. They argue this has changed: With the advent of social media opinions that people spout are easily linked back to the organization they work for.

   An anecdote to support this issue is: In one of the organizations, an employee told the world on Twitter that he had downloaded illegal material at work. A simple Google search led to his LinkedIn profile. The employee had not thought of the consequences: specific issues like these can impact the public image of an organization. Because in the public sector, the organizations are paid for with tax money this could not only lead to problems for the specific organization but for the government as a whole.

6 Future work

This chapter describes what future work can be done, based on this research. On one hand it will focus on flaws this research had, and on the other hand on interesting data that came out of this research, allowing for follow-up research.

6.1 *Improvements to this research*

Most improvements that could be made to this research stem from two issues:

- Lack of resources, time, etc. in this research project
- Lack of time of the interviewees

The first issue led to this research being on a relatively small scale, only doing a handful of interviews in a certain sector. With more resources, future work could include a larger project that spans several sectors and has a lot more data from different organizations. With a larger sample size, the data could be used for statistical analysis, instead of taking a qualitative approach. For example, a questionnaire could be made and sent to a larger number of organizations. However, doing more qualitative research would not yield many results. The interviewees within this research project had a very uniform opinion, and I highly doubt that more interviews would give different results.

The second issue led to another problem. Because the time with each interviewee was limited, the 133 ISO 27002 controls were grouped, ending up with 37 subtopics divided over 9 topics. These were then, as a questionnaire for each interview. The downside of this approach is that it is not possible to exactly know what controls are in use at certain organization. In an optimal situation, each of the 133 controls would be checked off at each organization. Therein lays a problem: It will be very hard, possibly impossible, to find people within organizations that are willing to spend a lot of time on such a research project.

6.2 *Follow-up research*

However, another approach to this research could be to take an even smaller subset of controls. E.g. only using controls that concern employees. That would allow a project that has the same resource constraints as this one to be able to analyze on a control level, instead of a subtopic level.

In this research, only the public sector was taken as a scope. It could very well be that other interesting sectors exist, e.g. the health sector or the financial sector.

A topic that might be worth investigating is **security awareness in the public sector**. In some of the organizations the average age of the employees was over 50. This means that

most employees did not grow up in the age of computers. According to the experts at the organization, this shows. The data from the questionnaire, which can be found in chapter 5.2, supports this. Unfortunately, it was not within the scope of this research project to investigate this further. Further research could focus on trying to find out why the culture in the public sector is not information security minded, and if/how this could be improved.

As mentioned in chapter 5.4, **social media** can do serious damage an organization's image. This creates a whole new problem: An organization needs to directly influence the culture of the employees. I can't help but wonder if this is possible, and how you should approach influencing a culture to make employees more information security minded.

Management commitment is, as is in many organizations, an issue for organizations within the public sector. However, for organizations in the public sector the situation is slightly different.

Whenever something goes wrong in the private sector, only the image of that organization is harmed. However, when something goes wrong in the public sector the **image of the national government** can be harmed, and politics can come into play. For example, the Dorifel virus and its impact were discussed by national politicians[9]. Therefore, an interesting question for follow-up research could be: Should the national government enforce information security management commitment for organizations that could harm the image of the national government?

[9] http://www.nu.nl/internet/2884531/sp-wil-debat-dorifelvirus.html

7 Conclusions

The goal of this research project was to discover in what way information security controls are selected. To reach this goal, five people who are responsible for information security within their organization were interviewed. These organizations represent all branches of local or provincial government.

The controls that those in charge of information security have brought into practice in their organizations can be seen in figure 6.

This does not always correspond with their ideal situations. Most of them wanted to improve on some controls, e.g. employees and security awareness but ran into issues with the organizations and therefore decided other controls would give the organization more better return on their time investment.

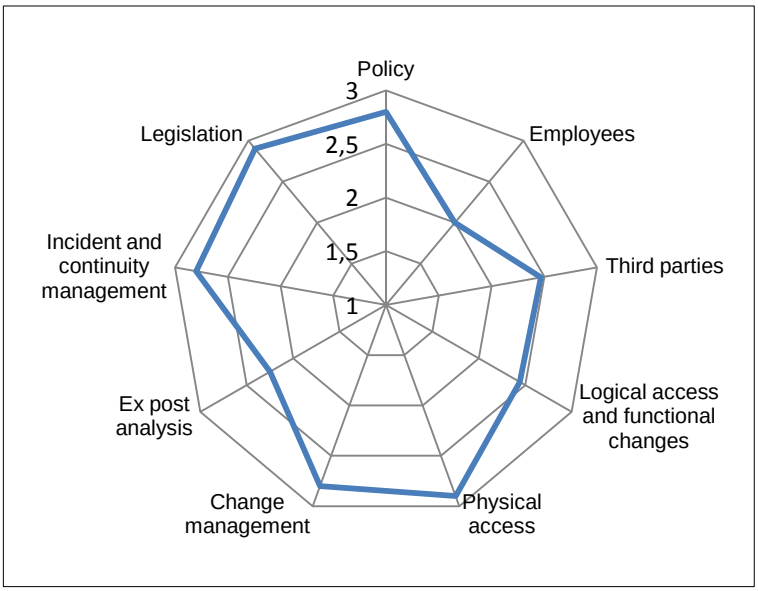


Figure 6: Overview of average scores on each topic

Selecting controls

1. For most of the organizations, the controls would be selected ad-hoc – using common sense. Often, a lot of 'controls' were implemented before ISO 27002 was used. For example, physical security has been an issue a long time before information was stored digitally.
2. Other organizations used an approach with expert interviews: By asking each of the experts within an organization, e.g. the director of facilities, the director of the IT department, etc. what their upcoming plans are to improve the information security.
3. One organization made a risk analysis for their controls by making a matrix of guesstimated risks and impact and created a plan for each of these.

Importance of controls

For ad-hoc approaches selecting controls, number one and two of the previous section, most interviewees did not have a good idea of the criteria they used to select some controls over others. By discussing some potential issues of an ad-hoc approach with them, they agreed with the statement that most controls were selected because:

- They were asked directly by employees
- It concerned business continuity

- They were forced to comply to certain legal demands

Approach to information security

Although some interviewees were operating on another level than other employees, e.g. more high level, e.g. management, or low level, e.g. most employees, the interviewees seemed to think that getting your organization committed to information security on all levels was vital. When the management has given an explicit commitment statement, most interviewees think a risk analysis should be the next step. This risk analysis should lead to a list of controls that should then be prioritized based on the risk/impact. Therefore, the interviewees think the most important controls are those that concern governing information security:

- Attaining management commitment (subtopic 1)
- Having an information security policy that the management has signed off on (subtopic 1)
- Having a continuity plan with redundancy and fallbacks; this was often cited as public sector organizations have to be able to service citizens(subtopic 33)

Noteworthy issues

Apart from the issues that I set out to investigate, two other issues came up spontaneously:

- The first issue is that the culture of employees in the public sector. Most interviewees said that their employees were not proficient at estimating security risks of their actions. Some of them argued this was due to the average age of the employees being around or above 50 – implying that these employees did not grow up with computers. Many of them would like more security awareness training, but the employees and/or the management did not feel the need for it.
- Another issue that most interviewees confirmed was the lack of management commitment and/or insufficient authority for the security officers. The interviewees often were part of the IT department, which would be problematic whenever they ran into non-IT security problems. They would either directly approach the department responsible for this problem, who would tell them it's none of their business or approach management who would be pre-occupied.

7.1 *Research merits and shortcomings*

This research project gives insight into the current information security situation in the public sector. As there is little scientific information on the state of ISO 27002 in that sector, this research project can provide insight into what issues the ones of in charge of information security have and what they think the best approach to information security is.

There are however some shortcomings. The biggest shortcomings stem from lack of time from both me and the interviewees. Because the time for each interviewee was limited to one

hour, a choice between covering all ISO 27002 chapters and tallying a fixed number of the 133 controls had to be made. A decision was made to cover all topics, losing the ability to list the specific controls that were used – going deeper than subtopic level is no longer possible.

Another choice that was made early was to select interviewees within the public sector, over for example the health sector. This choice was driven mostly by availability.

7.2 *Process and reflection*

In general, I think the research project has gone well. Given the fact that this research was meant as exploratory, I feel that it has given sufficient insight in what other research could focus on.

However, I might have underestimated some things. A lot more time than expected went into acquiring a list of possible interviewees and corresponding with them:

- Getting permission to use Ernst&Young client information. Both my research and proposal eventually were signed off by a Partner, making many revisions in between to make sure the quality was of the highest standard. In my opinion, there's nothing wrong with this approach. However, because of the amount of revisions and people needing to read / sign off on the documents, it took longer to get permission to contact clients than I expected in advance.
- Another thing that took longer than expected was communicating with possible interviewees. After I sent the letter, most of them did not respond right away. I would call them a few days after. Sometimes they would tell me right away whether they wanted to be part of this research, but sometimes they would first have to consult colleagues, usually during a meeting. This could take up to two weeks. Interviews could then be planned for 2-3 weeks ahead.

When the interviews were completed, I usually sent an interview report within a week. Sometimes the interviewees agreed with the report right away, but sometimes it took a couple of weeks, where small requests followed by small revisions were sent back and forth. The turnaround time was therefore occasionally more than 2 months.

These two things led to having fewer interviewees than expected in the research proposal. I feel that the interviews that were performed gave enough data to be able to draw conclusions, because the interviewees, who were part of all kinds of organizations – some small, some large, all gave a very uniform response. That is also supported by the questionnaire, where most interviewees scored similarly.

Originally, the idea was to tally specific ISO 27002 controls. After a while, though, I realized that the amount of time for each interview was more or less limited to one hour. As there are 133 controls in total, a choice had to be made: Either severely limit the number of controls – completely disregarding some topics or grouping controls, which would mean the questionnaire results would no longer be able to be mapped 1:1 to ISO 27002 controls, but would allow discussing every topic.

Obviously, the latter was chosen as I deemed it more important to cover every aspect of information security than to be able to count specific controls. My reasoning for this was that this research project was meant as exploratory research – drawing a high level map that further research could be based on.

7.3 *Personal recommendation*

My personal recommendation to the organizations included in this research is:

- Raise awareness amongst higher management. Most interviewees seemed to be aware of security issues within their organization, but the management did think it could be easily abused. Some organizations used mystery guests – professionals who video record their attempt to gain access to confidential information. Showing these videos seems like a good way to convince management that getting in can be done, and often rather easily.
- Too often information security is seen as an IT problem. Most organizations had their security officer as part of the IT department – sometimes giving problems when an issue had no clearly defined department. Because all the organizations are in the public sector, I would advise the national government to create a guideline in which it is clearly stated that information security is not an IT issue, and should therefore be handled by someone who is not part of the IT department. Instead, the security officer should only have to report to the management, and work together with different departments to improve information security.
- Improve security awareness amongst employees. This is however a very complex issue and I don't think there is a one-size-fits-all solution available. It would require an analysis of why people are not aware of information security. Are they just not informed? Do they think it's not important? A number of underlying problems need to be identified, and resolved. This possibly involves changing the culture within an organization – something that is hard and takes a lot of time.

8 Acronym list

Acronym	Meaning
IS	Information security
ISMS	Information security management system
SSF	The Software Security Framework
WOB	Wet Openbaar Bestuur. A Dutch law that requires all government organizations to be open. A request can be made to an organization to request certain information, and that organization is obliged to give this information.
CIBO	Centraal informatiebeveiligingsoverleg. A platform for all provinces to exchange information and ideas on information security.
KING	KwaliteitsInstituut Nederlandse Gemeentes. An organization that strives to maintain quality throughout all the municipalities.
GBA	Gemeentelijke Basisadministratie Persoonsgegevens. A database containing basic citizen information.
DigiD	A Dutch government system allowing citizens to authenticate themselves online for access to government systems.
NCSC	Nationaal Cyber Security Centrum.

9 Bibliography

Ernst & Young. (n.d.). *Global Information Security Survey.* Retrieved 12 3, 2012, from http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf

Gary McGraw, S. M. (2012, September). *BSIMM.* Retrieved from http://bsimm.com/download/

Gerber, M., & Solms, R. v. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security* , 124-135.

Höne, K., & Eloff, J. (2002). Information security policy - what do international information security standards say. *Computers & Security* , 402-409.

Polkinghorne, D. E. (2005). Language and Meaning: Data Collection in Qualitative Research. *Journal of Counseling Psychology , 52* (2), 37–145.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences* , 23-29 .

Taleb, N. N. (2001). *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets.* New York: Random House.

Verheul, E. (2011). *Introduction to information security Lecture #1.* Radboud University, Nijmegen.

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security. *The information management journal* , 371-376.

10 Annex A

Controls, interview checklist of controls

Annex A describes how important the controls in different chapters in ISO 27002 were viewed by experts at Ernst&Young.
Green is for ‘must include’, yellow for ‘could be included’ and red for ‘need not be included’.

Each chapter of ISO 27002 corresponds with a chapter below. For each chapter a interview topic, the objective of the chapter and the controls that belong to that chapter are noted.

10.1 *Chapter 5*

Interview topic: Information security policy is required and commitment needs to be shown by management.

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

10.1.1 Subcontrols

No.	Name	Summary	Implemented
1	Information security policy document	An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.	

2	Review of the information security policy	The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	

10.2 *Chapter 6*

Interview topic: A management framework(ISMS) should be made, including security roles and reviews. Contact should be maintained with external parties and authorities to keep up.

Objective: To manage information security within the organization. A management framework should be established to initiate and control the implementation of information security within the organization. Management should approve the information security policy, assign security roles and co-ordinate and review the implementation of security across the organization. If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists or groups, including relevant authorities, should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when handling information security incidents. A multi-disciplinary approach to information security should be encouraged.

No.	Name	Summary	Interview guidelines	y/n
1.1- 1.3	Management commitment to information security	Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions. All information security responsibilities should be clearly defined.	Checken of er een ISMS is. Verantwoordel ijkheden	
1.4	Authorization	A management authorization process for new information processing facilities should be		

	process for information processing facilities	defined and implemented.		
1.5	Confidentiality agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed.	WBP	
1.6	Contact with authorities	Appropriate contacts with relevant authorities should be maintained.		
1.7	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.		
1.8	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.	Third party agreements Awareness tegen social engineering? Hoe enerzijds omgaan met klantvriendelijkheid, anderzijds omgaan met mensen met slechte	
2.1	Identification of risks related to external parties	The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.		
2.2	Addressing security when dealing with customers	All identified security requirements should be addressed before giving customers access to the organization's information or assets.		

			intenties	
2.3	Addressing security in third party agreements	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.	SLA's?	

10.3 *Chapter 7*

Objective: To achieve and maintain appropriate protection of organizational assets. All assets should be accounted for and have a nominated owner. Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.

No.	Name	Summary	Interview guidelines	y/n
7.1.1	Inventory of assets	All assets should be clearly identified and an inventory of all important assets drawn up and maintained.	Informatiebronnen – welke zijn er aanwezig? Standaard open of standard dicht? USB Sticks, archief, backups, Vanuit een gebouw, wie kan waarbij?	
7.1.2	Ownership of assets	All information and assets associated with information processing facilities should be owned by a designated part of the organization.		
7.1.3	Acceptable use of assets	Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.		
7.2.1	Classification guidelines	Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.		
7.2.2	Information labeling and handling	An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization.		

10.4 *Chapter 8*

Interview topic: making sure people are aware of their responsibilities and possible information thefts.

Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment. All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs. Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities.

In/uitdienst en functieverandering

No.	Name	Summary	Interview guidelines	y/n
8.1.1	Roles and responsibilities	Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.		
8.1.2	Screening	Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.		
8.1.3	Terms and conditions of employment	As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.		
8.2.1	Management responsibilities	Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.		

8.2.2	Information security awareness, education, and training	All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.	Steeds belangrijker – mensen en niet technologie zijn vaker oorzaak van informatielekken	
8.2.3	Disciplinary process	There should be a formal disciplinary process for employees who have committed a security breach.		
8.3.1	Termination responsibilities	Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.	Bij be-eindiging contract, hoe wordt er gezorgd date r geen informatie tegen ze gebruikt kan worden?	
8.3.2	Return of assets	All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement.		
8.3.3	Removal of access rights	The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.		

10.5 *Chapter 9*

Interview topic: How is the physical security implemented?

Objective: To prevent unauthorized physical access, damage, and interference to the organization's premises and information. Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and

entry controls. They should be physically protected from unauthorized access, damage, and interference. The protection provided should be commensurate with the identified risks.

No.	Name	Summary	Interview guidelines	y/n
9.1.1	Physical security perimeter	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.	Hoe zorgt men ervoor dat men niet ongewenst binnenkomt?	
9.1.2	Physical entry controls	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.		
9.1.3	Securing offices, rooms, and facilities	Physical security for offices, rooms, and facilities should be designed and applied.		
9.1.4	Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.		
9.1.5	Working in secure areas	Physical protection and guidelines for working in secure areas should be designed and applied.	Wat valt er precies onder secure areas?	
9.1.6	Public access, delivery, and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Indien in deels openbare locaties gemeentes/provincies	
9.2.1	Equipment siting and protection	Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.		
9.2.2	Supporting	Equipment should be protected from power failures and other disruptions		

	utilities	caused by failures in supporting utilities.		
9.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.		
9.2.4	Equipment maintenance	Equipment should be correctly maintained to ensure its continued availability and integrity.		
9.2.5	Security of equipment off-premises	Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises	Thuiswerken?	
9.2.6	Secure disposal or re-use of equipment	All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	Hoe wordt bijv papier verwerkt? Oude harde schijven?	
9.2.7	Removal of property	Equipment, information or software should not be taken off-site without prior authorization.		

10.6 *Chapter 10*

Interview topic: Change management, logging and media policies.

Objective: To ensure the correct and secure operation of information processing facilities. Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating procedures. Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

No.	Name	Summary	Interview guidelines	y/n
10.1.1	Documented operating procedures	Operating procedures should be documented, maintained, and made available to all users who need them.	Change management SLA	

10.1.2	Change management	Changes to information processing facilities and systems should be controlled.		
10.1.3	Segregation of duties	Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Algemeen praatje: Hoe is het IT beveiligd?	
10.1.4	Separation of development, test, and operational facilities	Development, test, and operational facilities should be separated to reduce the risks of unauthorised access or changes to the operational system.		
10.2.1	Service delivery	It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.		
10.2.2	Monitoring and review of third party services	The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.		
10.2.3	Managing changes to third party services	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.		
10.3.1	Capacity management	The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.		
10.3.2	System acceptance	Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance.		
10.4.1.	Controls against	Detection, prevention, and recovery controls to protect against malicious code		

	malicious code	and appropriate user awareness procedures should be implemented.		
10.4.2	Controls against mobile code	Where the use of mobile code is authorized, the configuration should ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.		
10.5.1	Information back-up	Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.		
10.6.1	Network controls	Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.		
10.6.2	Security of network services	Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided inhouse or outsourced.		
10.7.1	Management of removable media	There should be procedures in place for the management of removable media.		
10.7.2	Disposal of media	Media should be disposed of securely and safely when no longer required, using formal procedures.		
10.7.3	Information handling procedures	Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.		
10.7.4	Security of system documentation	System documentation should be protected against unauthorized access.		
10.8.1	Information exchange policies and procedures	Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.		
10.8.2	Exchange	Agreements should be established for the exchange of information and software		

	agreements	between the organization and external parties.		
10.8.3	Physical media in transit	Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.	Verplaatsen van informatie.	
10.8.4	Electronic messaging	Information involved in electronic messaging should be appropriately protected.		
10.8.5	Business information systems	Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.	DigiD(!!)	
10.9.1	Electronic commerce	Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.		
10.9.2	On-Line Transactions	Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.		
10.9.3	Publicly available information	The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.		
10.10.1	Audit logging	Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.	Loggen wat er gebeurt, zodat zowel intern als extern gecontroleerd kan worden	
10.10.2	Monitoring system use	Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.		
10.10.3	Protection of log information	Logging facilities and log information should be protected against tampering and unauthorized access.		
10.10.4	Administrator and	System administrator and system operator activities should be logged.		

	operator logs			
10.10.5	Fault logging	Faults should be logged, analysed, and appropriate action taken.		
10.10.6	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.		

10.7 *Chapter 11*

Interview topic: Information access

Objective: To control access to information. Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements. Access control rules should take account of policies for information dissemination and authorization.

No.	Name	Summary	Interview guidelines	y/n
11.1.1	Access control policy	An access control policy should be established, documented, and reviewed based on business and security requirements for access.	Logische toegangsbeveiliging: Wie krijgt wanneer toegang?	
11.2.1	User registration	There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.		
11.2.2	Privilege management	The allocation and use of privileges should be restricted and controlled.		
11.2.3	User password management	The allocation of passwords should be controlled through a formal management process.		
11.2.4	Review of user access rights	Management should review users' access rights at regular intervals using a formal process.		
11.3.1	Password use	Users should be required to follow good security practices in the selection and use of passwords.		

11.3.2	Unattended user equipment	Users should ensure that unattended equipment has appropriate protection.	Medewerkers moeten hardware en software als goede huisvaders behandelen	
11.3.3	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.		
11.4.1	Policy on use of network services	Users should only be provided with access to the services that they have been specifically authorized to use.		
11.4.2	User authentication for external connections	Appropriate authentication methods should be used to control access by remote users.	Ook: mobiele devices.	
11.4.3	Equipment identification in networks	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.		
11.4.4	Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports should be controlled.		
11.4.5	Segregation in networks	Groups of information services, users, and information systems should be segregated on networks.		
11.4.6	Network connection control	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications.		
11.4.7	Network routing control	Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.		

11.5.1	Secure log-on procedures	Access to operating systems should be controlled by a secure log-on procedure.		
11.5.2	User identification and authentication	All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.		
11.5.3	Password management system	Systems for managing passwords should be interactive and should ensure quality passwords.		
11.5.4	Use of system utilities	The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.		
11.5.5	Session time-out	Inactive sessions should shut down after a defined period of inactivity.		
11.5.6	Limitation of connection time	Restrictions on connection times should be used to provide additional security for high-risk applications.		
11.6.1	Information access restriction	Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.		
11.6.2	Sensitive system isolation	Sensitive systems should have a dedicated (isolated) computing environment.		
11.7.1	Mobile computing and communications	A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.	!	
11.7.2	Teleworking	A policy, operational plans and procedures should be developed and implemented for teleworking activities.	Thuiswerken mogelijk?	

10.8 *Chapter 12*

Interview topic: Software development

Objective: To ensure that security is an integral part of information systems. Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements should be identified and agreed prior to the development and/or implementation of information systems. All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

Change management dekt het grotendeels

No.	Name	Summary	Interview guidelines	y/n
12.1.1	Security requirements analysis and specification	Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.		
12.2.1	Input data validation	Data input to applications should be validated to ensure that this data is correct and appropriate.		
12.2.2	Control of internal processing	Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.		
12.2.3	Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.		
12.2.4	Output data validation	Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.		

12.3.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information should be developed and implemented.		
12.3.2	Key management	Key management should be in place to support the organization's use of cryptographic techniques.		
12.4.1	Control of operational software	There should be procedures in place to control the installation of software on operational systems.		
12.4.2	Protection of system test data	Test data should be selected carefully, and protected and controlled.		
12.4.3	Access control to program source code	Access to program source code should be restricted.		
12.5.1	Change control procedures	The implementation of changes should be controlled by the use of formal change control procedures.		
12.5.2	Technical review of applications after operating system changes	When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.		
12.5.3	Restrictions on changes to software packages	Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.	Change management	
12.5.4	Information leakage	Opportunities for information leakage should be prevented.		

12.5.5	Outsourced software development	Outsourced software development should be supervised and monitored by the organization.		
12.6.1	Control of technical vulnerabilities	Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.	Pen testing	

10.9 *Chapter 13+14*

Interview topic: Incident management en continuiteit in het geval van een indicent.

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organizational assets. They should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. A business continuity management process should be implemented to minimize the impact on the organization and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities. The consequences of disasters, security failures, loss of service, and service availability should be subject to a business impact analysis. Business continuity plans should be developed and implemented to ensure timely resumption of essential operations. Information security should be an integral part of the overall business continuity process, and other management processes within the organization. Business continuity management should include controls to

identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

Wat is zoal een indicent?Diefstal, medewerkers, brand, etc etc.. continuiteitsplan, calimiteitenplan(ook voor informatie!)

No.	Name	Summary	Interview guidelines	y/n
13.1.1	Reporting information security events	Information security events should be reported through appropriate management channels as quickly as possible.	Voorbereidingen die getroffen zijn voor incidenten?	
13.1.2	Reporting security weaknesses	All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.		
13.2.1	Responsibilities and procedures	Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.		
13.2.2	Learning from information security incidents	There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	Zijn er eerdere incidenten geweest?	
13.2.3	Collection of evidence	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	Valt samen met logging en eerdere ervaringen.	
14.1.1	Including information security in the business continuity management process	A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.	Wat gebeurt er in het geval van een incident? Zijn er (kritieke)	

14.1.2	Business continuity and risk assessment	Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security.	bedrijfsprocessen die daarvan last ondervinden? Is dit meegenomen in de risicoanalyse?	
14.1.3	Developing and implementing continuity plans including information security	Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.		
14.1.4	Business continuity planning framework	A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.		
14.1.5	Testing, maintaining and re-assessing business continuity plans	Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.		

10.10 *Chapter 15*

<Misschien alleen WBP? Dit lijkt me een onderdeel waarover je uren kan praten..>
Interview topic: Legislatie etc.
Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements. Advice on specific legal requirements should be sought from the organization's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow).
Welke wet- en regelgeving gebruiken jullie? Hoe komen jullie daaraan? Externe partijen die controleren?

No.	Name	Summary	Interview guidelines	y/n

15.1.1	Identification of applicable legislation	All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.		
15.1.2	Intellectual property rights (IPR)	Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.		
15.1.3	Protection of organizational records	Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.		
15.1.4	Data protection and privacy of personal information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.		
15.1.5	Prevention of misuse of information processing facilities	Users should be deterred from using information processing facilities for unauthorized purposes.		
15.1.6	Regulation of cryptographic controls	Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations.		
15.2.1	Compliance with security policies	Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security		

	and standards	policies and standards.		
15.2.2	Technical compliance checking	Information systems should be regularly checked for compliance with security implementation standards.		
15.3.1	Information systems audit controls	Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes.		
15.3.2	Protection of information systems audit tools	Access to information systems audit tools should be protected to prevent any possible misuse or compromise.		

11 Annex B

Topic	Question / subtopic	Corresponding controls	
Beleid	Is er informatiebeveiligingsbeleidsdocument? Zijn de verantwoordelijken belegd bij de juiste personen? Is er draagvlak van het informatiebeleid door het management – ondertekend? Is er een security officer aangesteld – zo ja, heeft hij andere taken?	5.1 6.1.2 6.1.3	1
	Worden er nationale richtlijnen vanuit de overheid gebruikt?	6.1.6	2
	Wordt het beleid en de uitvoering daarvan onafhankelijk getoetst aan de hand van ISO 27001?	6.1.8	3
Personeel	Zijn er geheimhoudingsverklaringen? Zo ja, op basis waarvan?	6.1.5	4
	Zijn er security awareness trainingen? Zo ja, wat voor trainingen, hoe vaak, etc?	8.2.2	5
Externe partijen	Wordt er gebruik gemaakt van externe diensten, zoals schoonmakersbedrijven/servers op andere locaties/externe beheerders? Zo ja, hoe wordt de veiligheid gewaarborgd?	6.2.1 6.2.3 10.2.1	6
	Zijn er contractueel regelingen vastgelegd?	15.1.3 15.1.4	7
	Is er een plan over hoe informatie uitgewisseld wordt met andere gemeentes, overheid, ?	10.8.1	8
Informatieopslag/ en logische toegangsbeveiliging bij	Is er een inventaris van welke informatiebronnen welke informatie bevatten? Is er een eigenaar voor iedere informatiebron? Fysieke locatie, bij digitale bron: op welke server, wie mag toegang hebben?	7.1.1 7.1.2 7.1.3 7.2.1	9
	Hoe worden oude datadragers vernietigd? Oude pcs? Papier?	9.2.6 10.7.1	10

Indienst/uitdienst/ functiewijzigingen		10.7.2 10.7.3	
	Worden er backups gemaakt en getest?	10.5.1	11
	Hoe wordt er rekening gehouden met publieke informatie – websites, digid?	10.9.3	12
	Zijn de netwerken fysiek of digitaal gescheiden ingeregeld? Bijvoorbeeld, zitten baliemedewerkers op hetzelfde netwerk als de servers?	11.4.5 10.4.7	13
	Zijn er complexiteitseisen voor wachtwoorden? Is er aan de hand van een risicoanalyse bepaald hoe complex deze wachtwoorden moeten zijn?	11.3.1 11.5.3	14
	Is er een beleid voor hoe medewerkers hun computers behoren te behandelen en wordt hierop gecontroleerd?	10.4.1 10.4.2	15
	Is er ingeregeld wie welke informatie mag meenemen – fysiek uit archief? Hoe wordt er gecontroleerd dat dit juist gebeurt?	7.2.2	16
	Zijn er vaste procedures bij indienst met specifiek bepaling van welke toegangsrechten zij behoren te hebben /uitdienst inclusief inleveren van middelen en opheffen rechten? /functiewijzingen incl aanpassingen van rechten?	8.1.1 8.3.1 8.3.2 11.1.1 11.2.1 11.2.2 9.2.7	17
	Mogen medewerkers informatie meenemen? Denk aan USB-sticks, computers, fysiek uit archief? Wordt hierop gecontroleerd?	10.8.1 10.8.2 10.8.3	18
Fysieke beveiliging	Hoe is de fysieke toegang geregeld?	9.1.1 9.1.2	19

	Hoe zit het met deels openbare locaties? Gemeentehuizen ed?	9.1.6	20
	Is thuiswerken mogelijk? Zo ja, hoe wordt er gezorgd dat alleen medewerkers daar gebruik van maken? Zijn alle informatiebronnen te benaderen vanaf thuis?	9.2.5 11.4.2 11.4.6 11.7.2	21
	Is het mogelijk om mobiele devices die in beheer van de medewerker zijn mee te nemen (smartphones, tablets)? Zo ja, hoe wordt dit veiligheidsrisico afgedekt?	11.7.1	22
Software-ontwikkeling en change management	Is er een procedure omtrent het beheer van wijzingen? Als er nieuwe systemen ontwikkeld worden, is er een procedure om vast te leggen wat er precies ontwikkeld wordt – requirements, functioneel ontwerp, technisch ontwerp, etc.	10.1.1 10.1.2 12.5.1 12.5.2 12.5.3	23
	Aparte ontwikkel/test/productieomgeving? – evt acceptatieomgeving	10.1.3	24
	Penetration testing of andere praktijktesten?	12.6.1	25
Ex post-analyses	Wordt er gelogd?: voor Veranderingen van data buiten de applicaties – bijv door systeembeheerders direct op de database? Fouten en andere onverwachte gedragingen van system Wordt er standaard de logging gecontroleerd (proactief) of alleen wanneer er iets mis gaat(reactief)?	10.10.2 10.10.1 10.10.4 10.10.5	26
	Wordt er gecontroleerd of de logs niet handmatig zijn aangepast?	10.10.3	27
Incidenten en continuiteit	Is er een incidenten-meldpunt? Waar is die ondergebracht? Hoe worden incidenten gedocumenteerd?	13.1.1	28
	Kunnen daar ook zwakheden in fysieke of digitale beveiliging gemeld worden?	13.1.2	29
	Is er bepaald wat het management moet doen om een incident af te handelen?	13.2.1	30

	Wordt de impact van een incident naderhand bepaald, om te kijken of er geen onvoorziene gevolgen zijn opgetreden?	13.2.2	31
	Is er bepaald welke processen bedrijfskritisch zijn en welke systemen daarvoor gesteund wordt?	14.1.1 14.1.2	32
	Is er een plan bij uitval van die systemen? Fallbacks, andere locaties, etc?	14.1.3	33
	Worden die plannen up to date gehouden?	14.1.4 14.1.5	34
Legislatie en standaarden	Is er in kaart gebracht welke wetten van belang zijn? Zo ja, welke wetten? Bijv wet openbaar bestuur, wet bescherming persoonsgegevensp	15.1.1 15.1.2	35
	Worden er bepaalde standaarden nageleefd? ISO 27001?	15.2.1	36