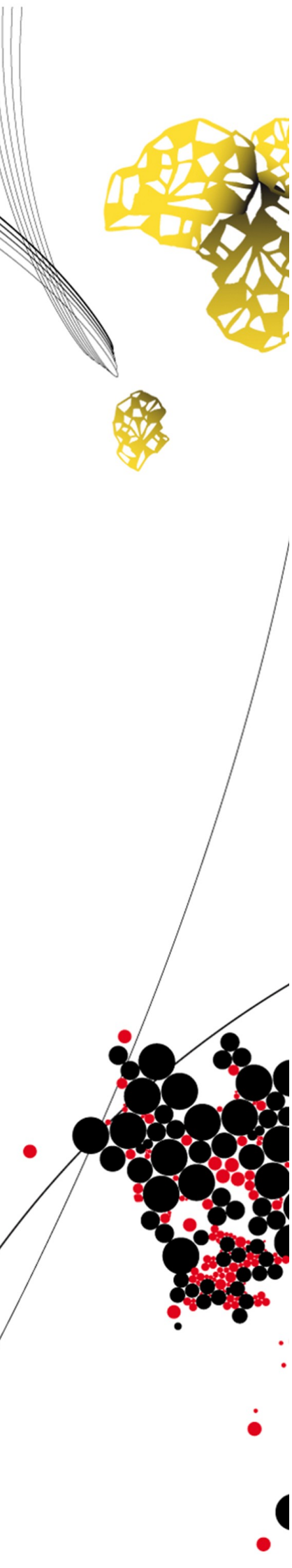


UNIVERSITY OF TWENTE.

Faculty of Electrical Engineering,
Mathematics & Computer Science

OSSUM - A Framework for Determining the Quality of Information Security Assessment Methodologies

Alexander Bakker

M.Sc. Thesis
July 2018

Supervisors:
prof. dr. M. E. Iacob
prof. dr. ir. M. J. van Sinderen

Telecommunication Engineering Group
Faculty of Electrical Engineering,
Mathematics and Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands

Preface

This is the preface of my master's thesis. As I'm writing it, I'm thinking of all of the things that I could have done better, at every stage, and whether all of the choices that I've made are the right ones. I am far from satisfied with it as it is, as I probably see the flaws that are in it better than most, since I'm the one that caused them.

Writing this master's thesis is without question the hardest thing I've ever done. I've dealt with uncertainty, stress and burnout symptoms, all the while feeling like what I'm doing is simply inadequate. The best way to describe what it felt like is trying to break down a brick wall by repeatedly bashing my head into it. And now, I've finally almost broken down the wall, and I'm going to give my head some well needed rest.

I am very grateful to my supervisors for guiding me along the way, and to Northwave, for the time and effort that they were always willing to invest in me. Finally, I am eternally grateful to my friends, my family, and my girlfriend Inge for supporting me while I was working on my thesis. Dear friends, thank you, as I could not have done this without the support that you have given me.

Summary

This thesis follows a literature study that was aimed at uncovering methods of measuring the level of Information Security within organizations, described in this thesis as Information Security Assessment Methodologies, or ISAMs for short. One of the main conclusions of the literature study was that only two of the 10 ISAMs identified were validated in practice. The literature concluded that there was to date no framework for validating ISAMs. This thesis aims to fill that gap.

In this thesis, a framework is presented that can be used to measure the degree to which an ISAM adheres to current standards. The framework generates a statistical overview of the ISAM, and can serve as a basis for improving the quality of ISAMs. The use of the framework is demonstrated by analyzing an ISAM called the State of Security assessment.

The framework developed in this thesis is called OSSUM, the Overarching Security Standard Unification Methodology.

Contents

List of acronyms

This chapter will contain all of the acronyms defined throughout the document, and will be filled while writing.

CMDB Configuration Management Database

CMM Capability Maturity Model

CSF Cybersecurity Framework

DSRM Design Science Research Methodology

FISMA Federal Information Security Management Act

GDPR General Data Protection Regulation

GLBA Gramm-Leach-Bliley Act

HIPAA Health Insurance Portability and Accountability Act

ICS Industrial Control System

ISAM Information Security Assessment Methodology

ISF Information Security Forum

ISMS Information Security Management System

ITIL Information Technology Infrastructure Library

NBS Northwave Business Security

NCS Northwave Cyber Security

NIST National Institute of Standards and Technologies

OCR Optical Character Recognition

OSSUM Overarching Security Standard Unification Methodology

OECD Organisation for Economic Co-operation and Development

OSCP Offensive Security Certified Hacker

PII Personally Identifiable Information

SOS State of Security assessment

SoGP Standard of Good Practice

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Information Security is rapidly becoming more important for organizations, pushed by forces like the increasingly complex IT landscape, a maturing cybercrime industry, an increasing focus on the importance of privacy by the public, regulatory pressure from governments, and an increased reliance of organizations on IT in their primary process. For this reason, being able to measure the level of Information Security within organizations is also becoming increasingly relevant.

While there are several industry standards that organizations can use in order to increase their level of Information Security, and get certified, fully implementing these Information Security standards may not be feasible for many organizations, for reasons like a shortage of budget. Yet other organizations do not feel the need to invest heavily in Information Security, because they feel that it is hard to justify such investments without a demonstrable return on investment.

For organizations that do not want to have a full auditing and accreditation process, and do not need to become accredited, it may be more beneficial to perform a measurement of the level of Information Security, or have this measurement performed by an expert organization. Such audits are usually less invasive and costly than a full implementation, and the insights of such a measurement can lead to tangible benefits at a reduced cost.

In an earlier literature study, several methodologies have been identified that can be used in order to determine the level of Information Security within an organization, which are collectively called Information Security Assessment Methodologys (ISAMs) in this thesis. One of the conclusions of the literature study, however, was that there was a clear need for a method of validating such methodologies, because most of the ISAMs discovered in literature were not validated in practice.

This thesis aims to fill this gap in literature by producing two results. First, a database is created containing all of the controls from a set of Information Security

standards, selected based on an earlier literature study. These controls are also categorized, which facilitates analysis of Information Security Assessment Methodologies. Second, a framework is created to apply the database in order to validate Information Security Assessment Methodologies.

By using this framework, the Overarching Security Standard Unification Methodology (OSSUM) framework, researchers will be able to demonstrate with a higher degree of confidence that the ISAMs they developed measures relevant Information Security standards. The suitability of the OSSUM framework is demonstrated by applying it to an ISAM used by the organization at which the author is performing his graduation.

1.2 Research questions

This section introduces the research questions of this thesis.

The main research question is as follows:

> What constitutes a framework for validating methodologies designed to assess the level of (aspects of) information security within organizations?

This is supported by the following subquestions:

1. Which standards, guidelines and other relevant materials should be covered by an Information Security Assessment Methodology?
   1.1. In which ways can the controls found in these standards be categorized?
2. How can Information Security Assessment Methodologies be validated according to relevant Information Security standards?

1.3 Thesis structure

The rest of this thesis is structured as follows. In chapter 2, some background is given that is needed for understanding the rest of this thesis. Among other things, this chapter explains the various Information Security standards that were found, and explains what an ISAM is. Chapter 3 outlines the methodologies used both in the earlier literature study, as well as in this thesis. The process by which the OSSUM framework was developed is detailed in chapter 4. Chapter 5 describes a case study that was performed using the OSSUM framework in order to demonstrate the feasibility of the framework. Finally, chapter 6 closes off this thesis, answering the research questions, providing a discussion about the results of this thesis as well as the limitations, and outlining potential future work based on this thesis.

Chapter 2

Background

This chapter will provide background information on information security, as well as leading Information Security standards.

2.1 Introduction to Information Security

Here, a definition will be given of Information Security. An overview of relevant Information Security standards will be given in 2.2, and a small introduction into relevant laws and regulations is given in subsection 2.2.6. Additionally, the area of Information Security is compared and contrasted with several similar but different areas.

Definition of Information Security

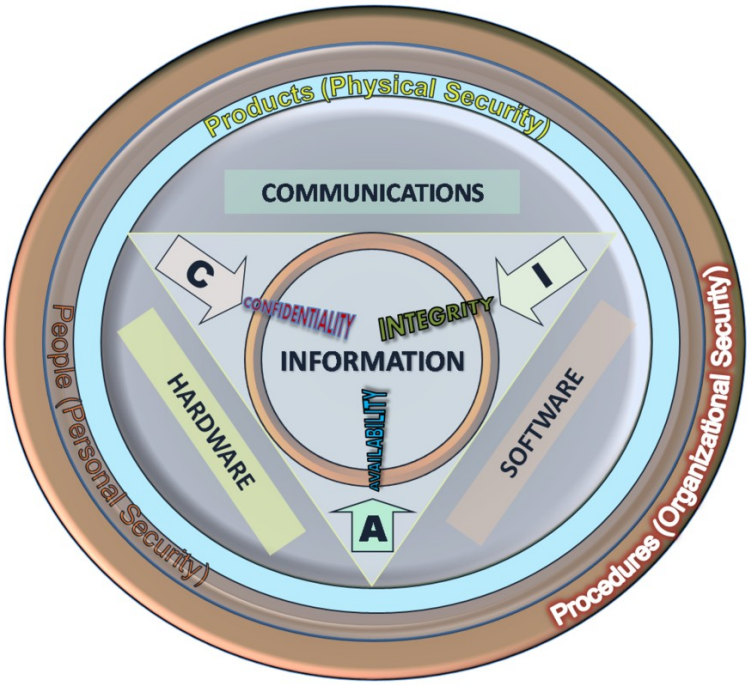
Information Security is a broad area that encompasses everything that has to do with protecting information within an organization. It is defined by the International Organization for Standardization (ISO) as:

> Preservation of *confidentiality, integrity and availability* of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved [35].

The generally accepted main components of Information Security are confidentiality, integrity and availability (sometimes also called the CIA Triad [60]), shown in 2.1. The interrelation between these terms is best described by the definition of Information Security by ISACA (previously known as the *Information Systems Audit and Control Association*) [27]:

> **[Information Security]** ensures that within the enterprise, information is protected against disclosure to unauthorized users (*confidentiality*), improper modification (*integrity*), and nonaccess when required (*availability*)

Figure 2.1: The CIA triad [74]



These elements are widely accepted throughout literature as core elements of information security, and virtually every definition of information security mentions at least these elements. Some extensions to this triad exist, such as the Parkerian Hexad [58], which extends the CIA triad with *possession/control* (of information), *authenticity* (which refers to the veracity of the claim of authorship), and *utility* (which refers to the usefulness of data in its current form).

The Organisation for Economic Co-operation and Development (OECD) instead developed nine generally accepted principles for the security of information systems and networks, which they recommend to any entity involved with an information system or network. These are awareness, responsibility, response (timely and co-operative response to threats and vulnerabilities), ethics (respect for legitimate interests), democracy (respect for democratic values), risk assessment, security design and implementation, security management, and reassessment [57].

A large number of laws, regulations, standards, checklists, guides, frameworks, tools and models exist in order to help or force organizations to achieve a satisfactory level of Information Security - so much so, in fact, that the sheer volume of material available, paradoxically, makes it hard to have an up-to-date understanding of the state-of-the-art. To paraphrase the Center for Internet Security [12]:

> Ironically, as defenders we have access to an extraordinary array of security tools and technology, security standards, training and classes, certifications, vulnerability databases, guidance, best practices, catalogs of security controls, and countless security checklists, benchmarks, and recommendations. (...) But all of this technology, information, and oversight has become a veritable ”Fog of More.”

Information Security is a fast-changing field, because of the rapidly changing nature of information technology, the new threats that arise as a result of those changes, and the organizational implications that some changes have. Some examples of new threats as a result of technological innovation are cloud malware as the result of cloud computing [37], information loss due to company laptops being taken off-premises [44], hackers gaining relatively easy access to devices used for Internet of Things applications [75], and adversaries having relatively easy anonymous access to cybercriminals through cryptocurrencies like Bitcoin [47].

2.2 Information security standards

Arguably the most well-established sources for Information Security are national and international standards on the topic [39]. As such, in this section, an short overview will be given of the relevant standards on the topic, their scope, and their history.

The definition of standard used in this section is *[S]omething established by authority, custom, or general consent as a model or example* [49]. Alongside self-described norms and standards, this also includes generally accepted best practices, checklists and other materials. The standards differ from each other in, among others, the scope of what they address (some address Information Security over the entire spectrum, whereas others specifically focus on cybersecurity), the method by which these standards aim to affect organizations (e.g. my means of a list of requirements, checklists, a maturity model, or a prescriptive method), their general acceptance (how widespread their use is), and their availability (free of charge, available for a fee, available with a membership subscription, or something else).

A thorough understanding of the relevant frameworks, standards, guidelines, checklists and other materials, as well as some assurance that all relevant materials are included, is important in order to ensure that all relevant areas are covered. However, many of the materials that are widely used in practice are not published in scientific journals, and therefore might not show up in a conventional literature search.

A survey of IT and security professionals in the United States reported that 84% of surveyed organizations use at least one Information Security Framework, with the

following frameworks being cited most often [17]:

- PCI (47%)
- ISO 27001/27002 (35%)
- CIS Critical Security Controls (32%)
- NIST Framework for Improving Critical Infrastructure Cybersecurity (29%)
- Other (3%)

According to the survey, the materials that were mentioned when participants filled out *Other* were the following:

- HIPAA (The Health Insurance Portability and Accountability Act)
- FFIEC (The Federal Financial Institutions Examination Council)
- HITECH (The Health Information Technology for Economic and Clinical Health)
- CIP (Not further specified, but the *U.S. Critical Infrastructure Protection* is assumed - this is also covered by NIST)
- Internally developed guidelines

For clarity and brevity, the format by which we will refer to standards from here on out is [Name of publisher or body] [identifier of the specific publication of standard if applicable]:[year of publication, if relevant - otherwise, the latest version is implied], for instance ISO 27001:2013.

2.2.1 ISO 27k series

The ISO/IEC 27000 family of standards, also colloquially known as ISO27k, are a large and growing series of standards developed, published and maintained by a joint effort of the International Organization of Standardization (ISO) and International Electrotechnical Commission (IEC). ISO 27000:2016 is the standard's leading document, and describes of the other standards in the family [35].

Except for the sector-specific ISO 27k standards, all ISO standards are universally applicable [65], but an operationalization step may need to be made before applying them, partly due to their one-size-fits-all nature. For instance, when applying the 114 controls in ISO 27002:2013, the organization needs to select which controls are applicable to the organization [34], and needs to identify whether any controls are missing.

ISO 27001:2013 [33] is the most well-known standard of the ISO 27k family [31], and contains the requirements of an Information Security Management System (ISMS). An ISMS is a high-level management instrument that aims to help organizations implement a framework for managing the security of information assets [35].

ISO 27001:2013 also contains an Annex A, which sets out controls and control objectives for increasing Information Security on a more operational level. These are derived from and directly aligned with the controls set out in ISO 27002:2013 [34], which provides implementation guidance for these controls.

Worldwide, there are over 1.6 million organizations that have an ISO 27001 certification [36].

2.2.2 NIST Special Publication (SP) 800-53 revision 4

The National Institute of Standards and Technologies (NIST) is a non-regulatory agency within the U.S. department of Commerce [53]. One of its series of publications is the NIST SP 800 series, which is a series of over 179 publications (of which 20 are labeled as a draft at the moment of writing) [54]. The NIST SP 800 series is mostly oriented towards technical issues [61], and is very useful when it comes to the implementation of single controls [42].

Arguably the most important document in the NIST SP 800 series is NIST SP 800-53 (version at time of writing is *revision 4* or *r4*), which provides a catalog of security and privacy controls, and a process for selecting controls to protect organizations against information security threats [51]. Although the publication is primarily intended to provide controls for federal information systems and organizations, it is also suited for use by non-federal organizations.

NIST SP 800-53r4 also briefly touches on the Risk Management Framework, which is further outlined in NIST SP 800-37 [55]. The core of this Risk Management Framework consists of a 6-step iterative approach to improving the Information Security of an information system [51]:

1. *Categorize* the information system based on a FIPS Publication 199 impact assessment. This entails categorizing the potential impact of a compromise in confidentiality, integrity and availability of data, on a scale of *low - medium - high*;
2. *Select* the applicable security control baseline based on the results of the security categorization and apply tailoring guidance;
3. *Implement* the security controls and document the design, development, and implementation details for the controls;
4. *Assess* the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome;
5. *Authorize* information system operation based on a determination of risk; and
6. *Monitor* the security controls in the information system.

The controls in the NIST SP 800-53r4 catalog have an indication of a baseline, which serves as an indicator for which controls to implement. Based on the *Categorize* step of the Risk Management Framework, more or less controls should be considered for implementation.

Finally, while it is possible for US federal organizations to become certified and accredited based on NIST SP 800-53r4, the NIST SP 800-53r4 does not provide a mechanism for organizations outside the US Federal government to get certified. That is, use of the NIST SP 800-53r4 is entirely voluntary for non-governmental organizations.

2.2.3 CIS Critical Security Controls for Effective Cyber Defense (SANS CSC)

The Critical Security Controls for Effective Cyber Defense are a publication of the SANS Institute, a research and education organization focused on information security and computer security operating worldwide. It consists of a set of cybersecurity controls that, when implemented, should reduce an organization's susceptibility to most pervasive attacks [63].

The SANS CSC mentions five critical tenets of any effective cyber defense system (paraphrased):

1. Offense informs defense: only use controls that stop real-world attacks
2. Prioritization: prioritize controls that provide the greatest risk reduction
3. Metrics: use metrics as a shared language to communicate the effectiveness of security measures between multiple parties within an organization
4. Continuous diagnostics and mitigation: to measure the effectiveness of current security measures
5. Automation: automate defenses for reliability and scalability

The controls are based on input and feedback from a large number of information security practitioners, and are based on real-world data. Their scope is limited to system and computer security, and for a large part the controls do not address human or organizational aspects. Where they do, the focus is also usually on technical skills.

The controls are grouped in three Families, namely System, Network and Application. Each control has a number of clear, actionable sub-controls. Each sub-control is either marked as Foundational or Advanced, and is worded as a clear, actionable goal. In addition, each control is accompanied by an explanation as to why this control is essential, and a paragraph explaining the tools and procedures needed to implement the control.

2.2.4 NIST Cybersecurity Framework

The US National Institute of Standards and Technology (NIST) is a non-regulatory agency of the US Department of Commerce [53]. Among their publications is the NIST Cybersecurity Framework (CSF), a voluntary framework that was developed through collaboration between the US Government and the private sector, based on industry standards and best practices, and aimed at protecting the United States's critical infrastructure [52].

The CSF is described as a set of industry standards and best practices to help organizations manage cybersecurity risks, and consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Core contains a set of activities, and references other national and international Information Security standards where applicable. The Core consists of five functions (Identify, Protect, Detect, Respond and Recover), divided into 22 functions, which in turn are divided into 98 subcategories, each of which mentions a set of informative references. The subcategories provide clearly actionable goals that can be verified, comparable to the controls in ISO 27001:2013 Annex A [43]. The informative references also point to controls mentioned in the SANS CSC, COBIT 5, NIST SP 800-53 revision 4, and ISA 62443-2-1:2009 and ISA 62443-3-3:2013, and can be used to map these controls to eachother through the high-level categories in the NIST CSF.

It should be noted that, while ISO 27001:2013 contains the explicit requirement that a management system is in place to safeguard Information Security, no such mechamism is required in implementing the CSF. It is also not possible to be certified against the CSF, and it is therefore harder to demonstrate compliance to third parties, which is one of the strong points of ISO 27001:2013.

2.2.5 Other noteworthy materials

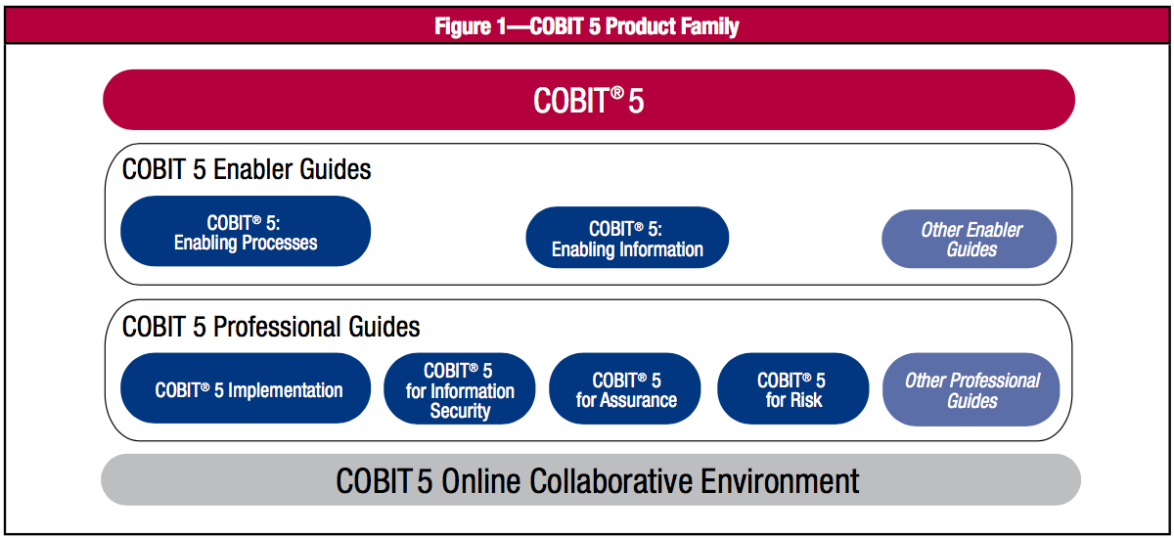
In this section, some other noteworthy materials are mentioned, that may or may not be useful. These materials are either tangentially related to information security, cover a subsection of information security, or don't meet the author's subjective, arbitrary notability requirements.

2.2.5.1 Control OBjectives for Information and related Technology (COBIT)

COBIT is a business framework for the governance and management of Enterprise IT. The most recent version of COBIT, COBIT version 5, was published in 2012, and is part of the COBIT 5 Product Family, which is shown in figure 2.2.

The COBIT 5 family of products contains, alongside the Framework itself, a set of Enabler guides, which discuss governance and management in detail, and a set

Figure 2.2: The COBIT 5 family of products [29]



of Professional guides, along with a collaborative online environment. One of these Professional guides is COBIT 5 for Information Security, which builds on the COBIT 5 framework in order to assist enterprises in achieving Information Security [30].

Although on the surface COBIT 5 for Information Security looks like a very interesting source, the full document was unfortunately not available for review to the researcher. Additionally, the process by which it was developed and the interrelationships between COBIT 5 for Information Security and other standards are not publicly disclosed, and no sources could be found to this effect.

2.2.5.2 ITIL

ITIL, formerly the Information Technology Infrastructure Library, is a best practices IT service management approach. It supports organizations in aligning IT services with business needs [3]. The best practices are detailed in five publications, each of which corresponds to one stage of the ITIL Service Lifecycle. The publications are:

1. ITIL Service Strategy [7]
2. ITIL Service Design [5]
3. ITIL Service Transition [8]
4. ITIL Service Operation [6]
5. ITIL Continual Service Improvement [4]

As ITIL is an IT service management approach, its scope is larger than merely Information Security. It does address the issue of Information Security as part of the publication ITIL Service Design [5], in which it bases its approach on the ISO 27001:2005 and ISO 27002:2005 standards, however because ITIL is structured as a set of best practices rather than a set of formal requirements (like ISO 27001 is),

it does not offer the same level of assurance. It should also be noted that the ISO standards that ITIL is based on have since been superseded.

2.2.5.3 (SSE)-CMM

Although focused on software engineering, not on Information Security, the Systems Engineering Capability Maturity Model (SECMM) is a process-maturity framework originally developed for software engineering, and is a tool by which organizations can measure and improve the level of maturity of specific areas within an organization [67]. The central concept of any maturity model is the idea of maturity, usually represented on a scale from less to more mature. The SECMM ascribes the following attributes to immaturity (slightly rewritten to pull away from the software development language used): reactionary, focused on solving immediate crises, regularly exceeding budgets because budgets are not based on realistic estimates, having no objective way to judge product quality or solve product or process problems. Conversely, it ascribes the following characteristics to maturity: possessing an organization-wide ability to manage [the process], employing managers that can accurately communicate [the process] to staff and new employees, and work activities are carried out according to the planned process. Mandated processes are usable and consistent with how work actually gets done, and get updated when necessary, supported by pilot tests and cost-benefit analyses. Roles and responsibilities are clear within a project and across the organization. There is an objective, quantitative basis for judging product quality and analyzing problems with the product and process.

In short, therefore, maturity contrasts with immaturity in a more formal, structured, consistent way of achieving more predictable results more efficiently, with an increased focus on continuous improvement.

The SECMM identifies five maturity levels (six, including level 0), ranging from least to most mature, defined as such:

0. Not performed
1. Performed Informally
2. Planned and Tracked
3. Well-defined
4. Quantitatively Controlled
5. Continuously Improving

Many other maturity models include maturity levels that are named similarly, and some omit the level ”0 - Not performed”, in essence merging it with level 1.

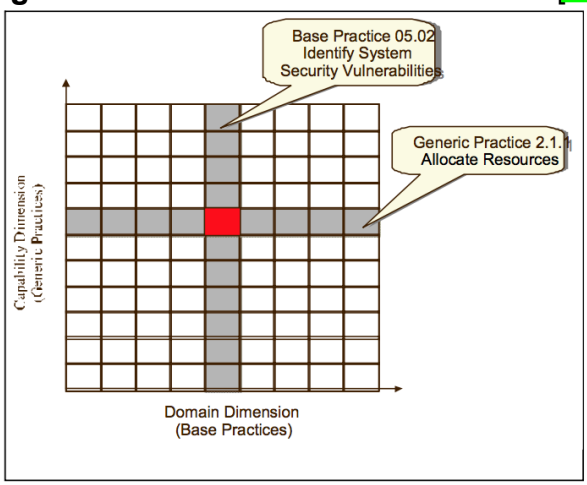
Another central notion in the SECMM is the concept of process areas (PAs), which are defined sets of related systems engineering process characteristics, which,

when performed collectively, can achieve a defined purpose. They consist of base practices, which are characteristics that must exist within the organization's process for the organization to claim satisfaction of that PA [67]. The SECMM defines 18 such PAs, which together encompass the base practices that are considered essential to the conduct of basic systems engineering.

The Systems Security Engineering Capability Maturity Model (SSE-CMM), originally developed by the International Systems Security Engineering Association (ISSEA), then published by ISO as ISO 21827:2002 and updated to ISO 21827:2008 [32], is a capability maturity model that is based on the SECMM. The SSE-CMM focuses on systems security engineering, which aims to ensure security throughout the systems engineering lifecycle. It has 129 base practices organized into 22 PAs, 11 of which are in the section "Security Base Practices", and 11 of which are in Annex B, "Project and Organizational Base Practices", which are adapted from the SECMM (SECMM PA 8 through 18). Some of the PAs are interrelated - for instance, PA03: Assess Security Risks relies on PA04: Assess Threat, PA05: Assess Vulnerability, and PA02: Assess Impact.

The basic model consists of a grid, with the Domain Dimensions (Base Practices) on one dimension, and the Capability Dimensions (Generic Practices) on the other. Answering all the questions raised by combining the Base Practices with the Generic Practices (such as Generic Practice 2.1.1 Allocate Resources with Base Practice 05.02 Identify System Security Vulnerabilities) will provide a good picture of the security engineering capability of an organization ("Does the organization allocate resources towards identifying system security vulnerabilities?").

Figure 2.3: The SSE-CMM basic model [32]



In order to evaluate the maturity of an organization, the maturity of the organization on each PA is judged. A maturity level within a PA can only be achieved if all of the previous levels have also been achieved, and the organization only achieves a

certain maturity level if all of the PAs have achieved that level. The reason for this is that all of the PAs have to have achieved a certain level in order for the organization to reap the full benefits associated with that maturity level.

While these models are aimed at (security) systems engineering, rather than Information Security, they have been used in several approaches that aim to improve Information Security. Tse [70], for instance, integrate ISO 9000 and BS 7799 onto the SECMM in order to create a Security Assessment Model for Information Security Practices. Goldman and Christie [22], meanwhile, combine ISO 17799 and the SSE-CMM in order to created a Metrics Based Security Assessment, a self-assessment tool for management to determine the level of maturity within an organization. Goldman and Ahuja [21], finally, integrate COBIT, the Balanced Score Card and SSE-CMM into an Information Security Management framework focusing on aligning business, IT and information security.

2.2.5.4 IASME

While 99.8% of all businesses in Europe are Small and Medium-sized Enterprises (having 249 or less employees [16]), there are very few frameworks, guidelines and standards that are specifically aimed at SMEs. Most standards are universal or generic in nature (like the ISO 27001:2013 standard, which can be applied to any organization), but for resource-constrained SMEs these standards may be too complex to apply effectively [24]. The IASME (Information Assurance for SMEs) standard [18] was developed in collaboration with the UK Government as a result of these findings, and is specifically aimed at organizations ”where spare cash is in short supply” [25]. It is based on ISO 27001, and is supplemented with ”ENISA, SANS [likely SANS Cyber Security Controls] and COBIT.” The UK Cyber Essentials information security good practices project is contained within the IASME standard.

Organizations can apply IASME using a self-assessment, which is verified by a certification body, after which they receive a certificate. Alternatively, organizations can apply for a certificate which includes a technical audit of their network and computers.

In applying IASME, the organization first has to establish its risk profile, classifying the organization’s risk profile as ”Low, Intermediate or Complex” based on the information technology footprint, value of information assets, and perceived motivation and technological capability of threat agents.

2.2.5.5 ISA 62443 (formerly ISA99)

The ISA/IEC 62443 series of standards (International Society of Automation and International Electrotechnical Commission, respectively; referred to from here on out

as ISA 62443 for brevity) is a series of standards designed with the goal of improving cybersecurity robustness and resilience into Industrial Control System (ICS) [26]. It builds on the ISO 27000 series of standards, which is focused on information security in organizations.

2.2.6 IS Laws and Regulations AKA legal compliance

In this section, a bird's eye view of laws and regulations pertaining to information security will be given. It is necessarily short and incomplete, partially due to time and resource constraints, the fact that the main author is not a lawyer,and the fact that an analysis of all laws and regulations falls outside of the scope of this literature study. Due to the geographic location of the author, this section focuses on European laws and Dutch laws, but because of the leading role that the U.S. plays in the field of Information Security, several relevant U.S. laws are mentioned as well.

There are not many laws that are related to information security. In general, the goal of information security is to protect the confidentiality, integrity and availability of data to organizations, and a compromise in this area essentially only hurts the organization itself. The laws that do pertain to information security aim to protect entities outside of the organization itself, who would be negatively impacted by a compromise of the CIA of certain data. Specifically, information security laws and regulations exist for the following areas:

- Protection of the privacy of individuals, specifically when pertaining to sensitive information
- Protection of classified information

The European General Data Protection Regulation of 2016 (GDPR; European Parliament and Council [20]. Dutch: Algemene Verordening Gegevensbescherming) is a law that enables individuals to better protect their rights with regards to their privacy, designed to be a single set of rules for all EU countries [15]. It applies to all organizations dealing with data on EU citizens, not just organizations located in the EU. It requires all organizations to notify the authorities of data breaches where a breach may "result in a risk for the rights and freedoms of individuals," gives individuals the right to demand confirmation as to whether data concerning them is being processed, and give the data subject a copy of the data free of charge upon request. It also gives individuals the right to be forgotten, or the right to have the data controller remove all data concerning them. Organizations that do not comply with the GDPR run the risk of incurring heavy penalties, of up to e 20 million or 4% of annual global turnover, whichever is greater. Organizations had until 25 May 2018 to comply with the General Data Protection Regulation (GDPR), which is the date on which it came into effect.

For the Dutch government (both on a national level and a municipality level), the Voorschrift Informatiebeveiliging Rijksoverheid 2007 (VIR; English: Regulation [on] Information Security [regarding] Civil Service) prescribes how the Dutch Civil Service is to secure information. Rather than a long list of checks and controls, the VIR simply states that management is to create a set of security requirements based on a risk assessment, to implement controls based on these security requirements, and to determine that the set of implemented controls adequately cover the established security requirements. A complementary set of measures is established to deal with sensitive information, called the VIRBI 2013 (BI stands for Bijzondere Informatie, or Special Information in English), which deals with data classification, among other things. Implementation of actual controls is done in accordance to the Baseline Informatiebeveiliging Rijksdienst 2012 (English: Baseline [for] Information Security [regarding] Civil Service), which is based on ISO 27001:2005 and ISO 27002:2005, and is based on the ”comply or explain” principle, which means that a control needs to be implemented, or an explanation needs to be given why the control is not implemented.

The U.S. plays a large role in the area of Information Security. Some of the leading materials on Information Security are created by departments of the U.S. government. The U.S. National Institute of Standards and Technology (NIST), for instance, publishes the NIST CyberSecurity Framework (CSF) and the NIST Special Publications 800-series on Computer Security. Three of the main federal cybersecurity regulations are the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Gramm-Leach-Bliley Act (GLBA) of 1999, and the Federal Information Security Management Act (FISMA) of 2002. Among other things, HIPAA aims to protect the privacy and security of Personally Identifiable Information (PII) related to health, by forcing organizations to put safeguards in place to protect the confidentiality and integrity of health information.

Another relevant piece of U.S. legislation in the area of Information Security is the USA PATRIOT Act. This law was passed following the 11 September 2001 terrorist attacks, in an effort to detect and prosecute terrorism. In combination with other laws, it gives U.S. law enforcement broad access to documents stored either in the U.S., or by U.S. organizations [46]. This is a factor that organizations should take into account when considering the confidentiality of their data.

2.3 ISAMs

As the goal of the framework described in this thesis is to analyze ISAMs, this section outlines what ISAMs are, and outlines the ISAMs that were found during the literature study. This section will conclude with an analysis of their theoretical foun-

dation, and argue the need for the framework that is developed in this thesis, as a way to established a more formalized way of validating ISAMs according to relevant Information Security standards.

2.3.1 What is an Information Security Assessment Methodology?

Information Security is not a new idea, and the concept of measuring Information Security is therefore also not new. This section introduces the term Information Security Assessment Methodology (ISAM), defined as *any framework or methodology that measures the level of Information Security within an organization, in whole or in part*.

The area of Information Security is an area in which things are sometimes referred to under different names. Information Security is sometimes referred to as Cybersecurity or Information Assurance, for instance.

The definition of an ISAM does not apply to tools or methodologies that aim to just measure the technical side of Information Security (a.k.a. Cybersecurity). An automated vulnerability scan, for instance, is not an ISAM by itself, although it can of course be part of an ISAM.

Finally, the word organization in the definition of ISAM is taken can be taken to mean one business, but it can also be taken to mean for instance a business unit, an entire supply chain or a government.

2.3.2 Overview of ISAMs

This section gives an overview of ISAMs found in literature, and is taken from the literature study.

2.3.2.1 History

Research into measuring information security is not new, but has come a long way, as demonstrated by von Solms et al. [71]. An Information Security Maturity Model (ISM^2) is proposed as a tool to manage information security. The model consists of a leveled description of 5 security situations in an organization (called Operational Security Environments, or OSEs). These are called the ideal, prescribed, baseline, current and survival OSEs. The paper does not clearly define what an OSE is, but implies that the level of Information Security can be adequately represented by a single level. Information Security is seen as one-dimensional, and can be categorized into physical, logical and personnel, which can then be further split up

into subcategories. The model that they use is very simplistic, and shows that the IT landscape has become much more complex since. This paper offers some historical insights, as it says that there are no clear international standards for Information Security yet. The need for such standards is evident from the lack of depth in the paper when compared to more modern papers.

Tse [70] give some insight in the state of information security in the year 2004. They give an overview of the leading information security frameworks of that time. Contrasted with von Solms et al. [71], there are already some information security models and frameworks. They also mention BS7799, the precursor to ISO 17799, which is an international standard. Also in contrast to von Solms et al. [71], the authors make a mention of the classical confidentiality, integrity and availability (CIA) triad, though interestingly the authors categorize all models and frameworks using the CIA triad in one group, which strongly implies that the authors did not yet see the CIA triad as the core of information security, as it is seen today. They also mention the Control OBjectives for Information and related Technology (COBIT) framework version 3 [28], even though it did not yet include a separate extension for Information Security (which came along in COBIT 5 [29]).

In addition, Tse [70] mention the Capability Maturity Model (CMM) as a framework for creating maturity models, and an extension of the CMM for systems security engineering, called the SSE-CMM. Tse [70] mention that this is only a consultative tool that is not clear enough to lead practitioners, and lacks an assessment mechanism. In order to remedy this, the authors create a new model by mapping the 10 sections in BS7799 onto the five levels of the Capability Maturity Model, although they have not validated the model in practice.

One example of a paper that focuses just on the security of IT, rather than Information Security as a whole, is Hallberg et al. [23], who created a framework to assess system security. Using their approach, first a model of the system is created, after which the elements of the system that generate traffic are used to calculate what the authors call the system-dependent security level. An Overall Security Level (OSL) is calculated. Their definition of IT security is upholding the CIA of information and services as provided by IT-based information systems with which the authors clearly indicate their belief that it is the responsibility of IT to uphold information security.

Chen et al. [14] advocate the use of workflow (”describing how a system performs its intended functionality”) as a basis for performing cybersecurity analysis. The method works by incrementally generating more specific flow graphs from higher level flow graphs by adding information about systems and attackers, and would lend itself to automating.

Indeed, the field of information security has often been criticized as taking too

much an IT-centric focus. Even today, organizations often look towards easy technological solutions to improve their information security, whereas in reality a magic silver bullet for Information Security is unlikely to exist. Although the security of information systems is obviously very important, because of the central role that information systems play in how organizations do business, focusing solely on IT overlooks the role that human and organizational factors play in Information Security.

One of the earliest methods to assess the level of Information Security organization-wide is found in a series of papers from Johansson and Johnson. Their approach is unique in that they explicitly recognize that an Information Security assessment cannot be performed with unlimited resources. They take the most representative standards in the area of Information Security at that time (ISO/IEC 17799, NIST 800-26, input from both the authors of the Information Security Forum (ISF) Standard of Good Practice and the OCTAVE framework, and a panel of experts at the Swedish Information Processing Society), and standardize the best practices found in those sources into a database of questions, categorized along the dimensions of time (planning, operating or controlling), purpose (responsive, detective or preventative) and scope (technical, organizational or environmental) [40]. These questions are then scored by a panel of experts on their relative importance in deciding the level of Information Security in an organization, and the relative amount of effort it takes to answer these questions [40]. They use this information, along with the principles to ask important and cheap questions above unimportant and costly questions, to select a set of questions to elicit the answers from, and calculate a single percentage score in a bottom-up manner. In this calculation, they also use heuristics to score the individual credibility of the answers of participants [39].

2.3.2.2 Metrics

The need for a more formalized method of calculating the level of information security is also identified by Wang [73], who note that security assessments are usually experimental and heavily based on the assessors experience, and that where metrics exist, they are usually qualitative and subjective.

Goldman and Christie [22] also mention that easy, quick technological fixes were in the past often used to respond to security issues, often without a lot of thought being put into their effectiveness. They, too, call for a use for metrics in information security assessments. In addition, they identify some weaknesses in ISO 17799. For instance, ISO 17799 is cited as being risk-independent, and this may lead to over- or under-investing; it does little to measure the effectiveness of investments; and it does not provide a high-level overview of itself, rather leaving that to the assessor. To overcome these issues, they map the ISO 17799 standard on the SSE-CMM.

Unfortunately, even though they mention that they use ISO 17799 and the SSE-CMM to cover each others weaknesses, they fail to mention any weaknesses in the SSE-CMM. Additionally, they do not publish the model that they created, nor the method by which they created it, in much detail, and they do not validate their model. The idea of mapping a well-known standard onto a maturity model to develop a new maturity model is sound, and their results would have been very interesting.

Breier and Hudec [10] also call for the use of more metrics in information security, specifically in the area of risk analysis, because of the subjectivity introduced into information security assessments by risk analysis who are influenced by their own knowledge and experience. In order to remedy this, they propose a risk analysis model based on the ISO27002:2005 control objectives.

While the application of metrics may be hard when it comes to enterprise information security, using metrics to improve IT security is very much feasible. Rudolph and Schwarz [62] observe that various IT security indicators have been proposed in literature, while few IT security metrics on their own have gained general acceptance. They gather and classify published IT security indicators, and organize them in a classification tree with as its top-level categories Cost (among which, for instance, the cost of a countermeasure), Probability (of an attack), Compliance (of a system or process, with relevant standards and guidelines), Target Coverage (fraction of security targets that satisfy a given security criterion), and Effectiveness/Rigor (for indicators that measure the effectiveness of countermeasures against attacks).

2.3.2.3 Maturity

The SSE-CMM proves to be a popular framework for adding the notion of maturity levels to other information security standards, as Goldman and Ahuja [21] prove by using it to combine the Business Scorecard [ref] and COBIT [ref] in order to create an information security management (ISM) framework. They note that it is oftentimes challenging for organizations to strategically integrate several frameworks, while the organizations that do successfully create an ISM framework can gain substantial value and benefits citing several studies that integrate ISO, ITIL and COBIT [ref]; ISO and SSE-CMM for a metrics-based assessment [ref]; and COBIT with ITIL and ISO 27002 for effective business-IT alignment [ref]. The integration of COBIT, BSC and SSE-CMM performed by Goldman and Ahuja [21] aims to create a framework that provides in aligning business, IT, and information security. In order to identify the strengths and weaknesses in creating an ISM framework, they perform a gap analysis between COBIT and BSC, although they dont mention how they gathered their list of problems. In addition, they mention that the model is not validated, and is just a conceptual model.

While there was certainly considerable research being done into Information Security around 2008, Mazhelis and Isomäki [48] point to the fact that this research was primarily focused on larger enterprises, and there were no adequate frameworks that were aimed specifically at small and medium enterprises. They make the observation that the set of frameworks that is in existence can be roughly split up into two groups: checklists and tailored methods. Checklists assume that organizations are similar enough that roughly the same set of actions is adequate for most of them, whereas tailored methods treat each organization as unique. Some frameworks strive to combine both approaches. Furthermore, they make the observation that even the smaller frameworks are not usable in small enterprises due to their wide scope and complexity. In order to remedy this, they adapt the OCTAVE-S approach, which is aimed at organizations of roughly 100 employees, to organizations of roughly 50 employees. The method that they used consists of three phases:

1. Asset-based threat analysis.
2. Assessing current situation and complementing existing mitigation activities.
3. Specify concrete to-do items.

They applied this method in an organization of roughly 50 employees and found that it performed well.

In comparing the most widely used frameworks at the time, Siponen and Willison [65] categorize existing frameworks in three categories: universal (applicable to every organization), generic (applicable through all organizations, with rare exceptions where it is not), or company-specific (recognizing that every organization may have unique requirements). In comparing BS7799 and its derivative ISO/IEC 17799:2000, GASSP/GAISP, and the SSE-CMM, Siponen and Willison [65] observe that these methods are all either generic or universal. In addition, Siponen and Willison mention that these frameworks are all validated by authority and practice, claiming that this is not a sound basis for a standard (although they fail to mention what a sound basis for validation would look like). They mention that every guideline should be company-specific, to a degree, because otherwise important company-specific requirements could fall by the wayside. In addition, they call for the creation of a library of information security guidelines (comparable in concept to the database of information security questions as used by Johansson et al. [41]), which outlines for each area the objectives, principles, cautions, key references and the type of evidence supporting each, for the use of information security practitioners.

Investments in cloud computing are continuing to grow as companies are increasingly moving towards the cloud. While evidence exists that cloud computing brings great advantages to those organizations that effectively adopt it, cloud computing is not without security implications, and these implications have to be

appropriately addressed by security standards. Ristov et al. [61] argue that ISO 27001:2005 (which has since been superseded with ISO 27001:2013) certification might not be enough for cloud service providers and cloud customers due to risks like multi-tenancy virtualization and data outsourcing, and propose an extension to ISO 27001:2005 for virtualization management.

Taylor [69] argues that current methods of information security assessment are flawed, because management decisions are often based on heuristics and optimistic perceptions. While not proposing a solution of its own, it does argue that there are problems with both quantitative methods (which may not include all necessary variables) and qualitative methods (which tend to yield inconsistent results). In addition, it argues against using metrics like the Annualized Loss Expectancy (ALE), Expected Loss (EL) and the Security Breach Probability Function (S), because these metrics all assume that decision makers can calculate the risk of a security incident, the damage should an incident occur, the countermeasures required to mitigate the risk, their cost and effectiveness, and/or the level of vulnerability in an organization. Additionally, it is hard to quantify intangible damage like loss of reputation.

2.3.2.4 Traceability matrix

In this section, a traceability matrix is given that shows which frameworks and standards are used in which papers, shown in table 2.1. This table shows the papers under consideration for this literature review, what the paper aims to produce, and whether they validated their results, as well as which standards and frameworks the end product is based on. The acronyms used are: Framework (FW), Management (MGMT), Information Security (InfoSec), Enterprise Information Security (EIS), Security (Sec), and Small and Medium Organization (SMO).

It should be noted that BS 7799 and ISO 17799 are both predecessors of the ISO 27000 series of standards. This explains, in part, why the ISO 27000 standards are used so little in the papers that were found.

Another striking insight is that only two of the methods found were validated in practice: Johansson and Johnson [40], who applied the framework by using it at a large electric utility company to assess the level of Enterprise Information Security, and Mazhelis and Isomäki [48], who applied their method in a SME research organization to help plan and assess information security. The OCTAVE method by Alberts and Dorofee [1] is an exception, in that this method is literally the OCTAVE standard - this standard has been used in practice extensively, but practical validation is not part of this paper per se.

Yet something else that stands out is that there are only 4 methods that use multiple standards, and that there are quite a few methods that use one standard

Table 2.1: Traceability Matrix - Frameworks per paper

Paper	von Solms et al. [71]	Alberts and Dorofee [1]	Tse [70]	Hallberg et al. [23]	Johansson and Johnson [40]	Wang [73]	Goldman and Christie [22]	Mazhelis and Isomäki [48]	Goldman and Ahuja [21]	Breier and Hudec [10]	Ristov et al. [61]
Goal of paper	InfoSec MGMT FW	OCTAVE	InfoSec maturity model	System Sec FW	EIS assessment method	System Sec FW	InfoSec Maturity FW	SMO Sec planning; assessment	InfoSec MGMT FW	Sec Evaluation Method	ISO 27001 for Cloud extension
Validated?	No	-	No	No	Yes	No	No	Yes	No	No	No
COBIT									X		
BSC									X		
CMM			X								
SSE-CMM							X		X		
CRAMM	X										
ISO 9000			X								
BS 7799			X								
ISO 17799			X		X		X				
ISO 27001											X
ISO 27002										X	
NIST SP 800-26					X						
OCTAVE					X						
OCTAVE-S								X			
ISF Standard					X						

only. This points to the need for a methodology to validate ISAMs according to multiple standards.

Chapter 3

Methodology

This section outlines the methodology of the literature search, as well as the methodology used during this study. It also gives a brief introduction of the Design Science Research Methodology (DSRM) [59], and explains how this paper maps to the different activities identified in the DSRM.

3.1 Literature search

Prior to starting the main phase of the graduation project, a systematic literature study was conducted. The results of this systematic literature study were used as inputs to this master thesis.

The main research question of the literature study was:

> Research Question 1: What measurement instruments are found in literature to measure the level of Information Security within organizations, and which standards are they based on?

Supporting this research question was the following question:

> Research Question 2: Which Information Security standards, frameworks and guidelines are widely used in practice?

In order to answer the first research question, a literature review was conducted according to the Systematic Literature Review methodology of Okoli and Schabram [56]. This methodology follows these steps:

1. **Purpose of the literature review**: Be clear and explicit about the purpose and intended goals of the literature review.
2. **Protocol and training**: For collaborative reviews, the reviewers need to agree on a protocol, and all reviewers need to be trained in this protocol in order to ensure a consistent process. *This step is skipped, because it mostly applies to collaborative reviews.*

3. **Searching for the literature**: Be explicit, explain and justify how comprehensiveness is ensured.
4. **Practical screen** (a.k.a. *screening for inclusion*): Be explicit about which studies are considered further, and which are eliminated without further examination, as well as the practical reasons for eliminating them.
5. **Quality appraisal** (a.k.a. *screening for exclusion*): Be explicit about what the criteria are for judging which articles are of insufficient quality to be included in the review synthesis. All articles need to be scored on their quality.
6. **Data extraction**: Systematically extract the applicable information from each study.
7. **Synthesis of studies** (a.k.a. *analysis*): Combine the facts from the studies using appropriate techniques (whether qualitative, quantitative, or both).
8. **Writing the review**: Adhere to standard principles of scientific writing, and ensure that the results of the review can be independently reproduced.

The *purpose of the literature review* step was concluded with the drafting of the research questions. Step 2, *protocol and training*, was skipped because this mostly applies to collaborative reviews. *Searching for the literature* (step 3) was done by developing and testing a set of keywords, using them to search for literature on scientific literature database Scopus [19], and exporting the results to a spreadsheet for further processing, yielding 418 results after refining the search terms. Furthermore, a Google Scholar search was conducted in order to ensure that all relevant literature has been found. After enriching the dataset with the data found in Google Scholar an initial set of 473 papers was found.

In the *Practical screen* step (step 4), papers were screened for inclusion. The inclusion criteria were:

1. The paper is likely to contribute to answering the literature review research question.
2. The paper deals with Information Security in organizations or relates to it.

Papers were filtered by first judging the titles based on these criteria (filtering out 352 as *"Not interesting"*), with 80 more papers being filtered out as *"Not interesting"* based on a review of the abstract. This left a set of 53 papers that were subjected to quality appraisal and a full-text review.

During the *Quality appraisal* step (step 5), several more papers were filtered out due to concerns about quality. Of the original 53 papers, 16 were not available for download, and a further 17 were filtered out because they were not applicable in hindsight. Furthermore, one more paper was filtered out because of quality concerns that were not apparent from the title and abstract alone.

In the *Data extraction* step (step 6), relevant information was extracted from the papers. A matrix was made of all papers, their stated contribution, whether this contribution was validated in practice, and which frameworks they based their research on. The set of frameworks that was extracted from these papers also served as the basis of the answer to Research Question 2.

During the *Synthesis of studies* step (step 7, a.k.a. *analysis*), the papers were first individually summarized, and an overall analysis was written in order to outline the similarities, differences and dependencies. This, along with the matrix that was developed during the *Data extraction* step, answered Research Question 1.

Finally, the literature review was finalized and turned into a coherent whole during the *Writing* step (step 8).

3.2 DSRM approach

Since the aim of this research project is to design a framework, it is appropriate to adopt a methodology that guides the process of creating artifacts. In this section, the DSRM by Peffers et al. [59] will be explained, and a justification will be given for selecting this methodology. Furthermore, a mapping will be given between Peffers' DSRM and this thesis.

3.2.1 Introducing Peffers' DSRM

Information Systems research is a relatively young area of research, which has developed rapidly over the last 30 years [2], and there is still ongoing debate about what exactly are the core theories of Information Systems research [50]. Additionally, while Information Systems is a very applied field, the scientific methods used to produce and publish Information Science papers have long been the same as those used in more descriptive areas of research, like physics (which attempts to describe natural phenomena) and psychology (which attempts to analyze human nature). Additionally, as [59] mentions:

> Information systems is an applied research discipline, in the sense that we frequently apply theory from other disciplines, such as economics, computer science, and the social sciences, to solve problems at the intersection of IT and organizations. However, the dominant research paradigms that we use to produce and publish research for our most respected research outlets largely continue to be those of traditional descriptive research borrowed from the social and natural sciences.

In many areas of science (for instance, in physics or social science), the focus is often on describing the real world around us. In contrast, the field of Information Systems is an applied field of science, which means the focus is not on describing objective truth, but rather applying sound principles in order to solve problems.

Peffers et al. argue that the research paradigms used in more descriptive fields of study are inadequate for design problems, which comprise a large part of the Information Study field. This leads to problems in the production of papers, as researchers lack a clear framework to structure their work, and in the interpretation of papers, since Information Systems researchers lack a mental model of a design science research approach.

Peffers' approach consists of a process model consisting of six activities. These activities are:

1. **Problem identification and motivation.** Define the specific research problem and justify the value of a solution.
2. **Define the objectives for a solution.** Infer the objectives of a solution from the problem definition and knowledge of what is possible and feasible.
3. **Design and development.** Create the artifact.
4. **Demonstration.** Demonstrate the use of the artifact to solve one or more instances of the problem.
5. **Evaluation.** Observe and measure how well the artifact supports a solution to the problem.
6. **Communication.** Communicate the problem and its importance, the artifact, its utility and novelty, the rigor of its design, and its effectiveness to researchers and other relevant audiences, such as practicing professionals, when appropriate.

The authors demonstrate the use of the DSRM by retroactively applying it to four already published Information Systems research projects, and how the projects are consistent with the activities prescribed in the DSRM [59].

Another method for conducting research in which an artifact is created for use in an organization is Action Research, which is a systematic approach to investigation that uses continuing cycles of investigation to generate effective solutions to real-world problems experienced in specific situations, often within the context of organizations [68]. However, the focus of Action Research is usually to develop an artifact to be used by the organization itself, in a collaborative manner with the participating group [66]. While most Action Research seems to consist of multiple iterations, this is not necessary - for instance, an approach with only one iteration is called linear AR by Baskerville and Wood-Harper [9].

Another widely used approach to Design Science, which marries it to Action Research, is Action Design Research, developed by Sein et al. [64]. It gives more

Table 3.1: Mapping this thesis to Peffers' DSRM

Chapter	Mapping to DSRM
1 - Introduction	1 - Problem identification and motivation
2 - Background	-
3 - Methodology	-
4 - Creating the framework	2 - Define the objectives for a solution 3 - Design and Development
5 - Case Study	4 - Demonstration
6 - Conclusions and recommendations	6 - Communication
7 - Discussion	6 - Communication

focus on the organizational context in which an artifact is to be used, and advocates an iterative process in which the artifact is released in incremental versions to the organization, after which the organization can use the artifact for their benefit and give feedback to improve the artifact.

Peffers' DSRM was chosen over other approaches because, while the artifact is to be used by organizations, it is not used in the primary process. Additionally, iterative development is unfeasible for time and resource constraints. The Evaluation step (5), which involves comparing the objectives of [the] solution to actual observed results from use of the artifact in the demonstration [59], is not made explicit in one specific chapter, but chapter 6 revisits the research questions and comments on how they are answered. Finally, among other things the Communication step (6) requires communicating everything that is appropriate to relevant audiences. While it is necessary to have access to the Database of Controls for application of the methodology, some of the sources (most notably the ISO 27001:2013 and ISO 27002:2013 standards) cannot be made public for copyright reasons. For this reason, a version of the Database of Controls will be made public which contains just the structure, which will require the researcher to add the content of the ISO 27001:2013 and ISO 27002:2013 standards for themselves.

3.2.2 Mapping Peffers to this thesis

This section demonstrates a mapping between this thesis and Peffers' DSRM, in order to demonstrate that all of the steps are taken. Table 3.1 shows each chapter of this thesis, and the activity or activities in Peffers' DSRM that it maps to.

Chapter 4

Creating a framework for validating ISAMs

This chapter outlines the process that was followed and the considerations that were made while designing the OSSUM framework. It starts with what the requirements are for the OSSUM framework. It gives a top-down view of how the OSSUM framework is supposed to work.

Then, the selection of standards is discussed, looking back at the background (section on Information Security standards).The process of filling the database is explained. The structure of the database is outlined. Finally, the method of applying the framework using the database is outlined.

4.1 Designing the OSSUM framework

This section outlines the steps taken in developing the OSSUM framework, and where applicable, points to the parts in this thesis where those steps are explained in more detail. These steps aim to fulfill activity 3 of the DSRM, Design and Development.

The steps taken in designing the database are as follows:

1. Develop requirements for framework. *See 4.2*
2. Select standards. *See 4.3*
3. Encode standards into database. See 4.4
4. Select categorizations. See 4.4.3
5. Trace controls to categories. 4.4.3
6. Develop method of tracing an ISAM to these controls. See 4.5
7. Develop method of analyzing and reporting the results
8. Report the results

4.2 Requirements for the framework

Before actually developing the OSSUM framework, first a set of informal requirements was drawn up. These requirements were decided upon jointly by the author and the product owner of the State of Security assessment (SOS). The Research Questions (see 1.2) can be considered very high-level requirements, and the requirements in this section were intended to provide a bit more guidance in developing the OSSUM framework.

The framework:

1. Should contain all relevant standards. *Note: a further analysis of relevant standards is provided in 2.3, and the selection of standards is discussed in 4.3*
2. Should encode controls correctly. All controls of the selected standards should be in the database, in a single uniform format.
3. Should categorize all controls adequately.
4. Should help in analyzing an ISAM for completeness, by allowing the researcher to trace between the ISAM and various controls.

With regards to the categorization of controls, some inspiration was drawn from Johansson and Johnson [38]. During the process of designing a database of questions regarding Information Security, in which the questions were derived from authoritative Information Security standards, they have developed a method of categorizing the controls according to three different dimensions, with three categories for each:

1. **Scope** (i.e. answer *how* the protection is implemented). Choice between *technical*, *organizational* and *environmental*.
2. **Purpose** (i.e. answer *why* the protection is carried out). Choice between *preventive*, *detective* and *responsive*.
3. **Time** (i.e. answer *when* the protective actions is carried out). Choice between *planning* (before), *operational*(during) and *controlling* (after).

A point of criticism on Johansson and Johnson [38] is that, even though the rest of their work relies heavily on this categorization, no explanation is given about how the dimensions came about. Nevertheless, their idea of categorizing the controls may provide greater insights into the standards themselves, as well as any ISAM implementing them.

In section 4.4.3, the process of selecting a categorization is explained, as well as the method of categorizing controls.

4.3 Selecting standards

International and national standards are, arguably, the most well-established sources with regards to Information Security [41]. Nevertheless, there is no one-stop all-purpose Information Security standard that serves all purposes. In the past, the precursor to ISO 27001:2005 (ISO 17799), has been criticized for being ”a mile wide and an inch deep” (Goldman and Christie [22] citing Walsh [72]; Cartwright [11]). Criticisms of the Cybersecurity Framework (CSF) include the fact that it is voluntary [45], and that it is not possible to certify against it. Furthermore, it does not go into great detail and leans heavily on other standards such as ISO 27001 and NIST SP 800-53. The latter is a very heavy-handed catalog of security controls that is primarily intended for use by the government of the U.S.

An approach used often by researchers and practitioners is to combine multiple sources of standards into one approach, for instance to alleviate perceived weaknesses of the individual standards. Tse [70], for instance, combined ISO 17799, BS 7799, ISO 9000 and the Capability Maturity Model (CMM) to create an Information Security maturity model, while Johansson and Johnson [39] combined ISO 17799, NIST SP 800-26, OCTAVE and the Information Security Forum (ISF) Standard of Good Practice (SoGP) to form an Enterprise Information Security assessment methodology.

In order to create a framework leveraging the state of the art of Information Security, the selection of standards is an important part. This step is complicated by the fact that there is little research comparing and contrasting Information Security standards, which makes comparing standards harder. From the 4 papers in the literature study that were published after 2005 (the first version of ISO 27001), only two referenced either ISO 27001:2005 or ISO 27002:2005: Breier and Hudec [10] while developing a Security Evaluation Model, and Ristov et al. [61] while developing an extension of ISO 27001 for the Cloud. Goldman and Ahuja [21] mention the importance of ISO 27001 but do not explain why they left it out, and Mazhelis and Isoräki [48] mention a large list of Information Security standards while omitting the 27000 series altogether. There does not appear to be one go-to standard in literature.

First, a list of potential Information Security standards was compiled, based on literature and other available sources. This list was prioritized based on what was found in literature, accompanied with experience from several experts in the area of Information Security.

Section 2.2 gives a more in-depth analysis of each individual standard.

Several standards and frameworks were classified as essential, with some more being classified as nice-to-haves.

The criteria that were used to determine which standards were selected were the

following:

1. The standard can be considered an industry default based on literature.
2. The standard ”adds to the mix,” for instance by having a different scope.
3. The standard adds something to the organization that the author is performing his research at.

The following standards were selected:

- ISO 27001:2013 and ISO 27002:2013, as they are the de facto standards and are universal in scope, meaning they apply to all organizations.
- NIST SP 800-53 rev 4 is the most extensive catalog of Information Security controls that could be found.
- The CIS Controls were initially a nice-to-have. The decision to include them was taken primarily because it is comparatively actionable.

Other standards were not included for various reasons. Other nice-to-have standards included PCI-DSS, SoGP, ISA 62443, Information Technology Infrastructure Library (ITIL), IASME and COBIT (see 2.2 for a summary of each, and more extensive reasons for excluding). Reasons for excluding them were lack of notability (SOGP, IASME), lack of focus on security (ITIL, COBIT), a specific focus on a limited subset of information security rather than an organization-wide scope (IAS 62443, which focuses primarily on IACS), and lack of time and resources (applicable to all).

4.4 Filling the database

In order to validate ISAMs using a multi-standard approach, it is important to have a single database of controls to use as the basis for validation. This section explains the process by which the standards were combined into one such database, and the choices that were made while combining them. First, this section outlines the structure of controls in the individual standards. Then, the section explains how the standards were encoded into one database, and how they were combined into one set. Finally, the section finishes with an explanation of why and how the controls were categorized, in order to facilitate analysis of ISAMs.

4.4.1 Structure of controls

This section explains the structure of the individual controls that make up the standards that went into the database. For a more extensive analysis of the standards, please see section 2.2.

4.4.1.1 ISO 27001:2013 and ISO 27002:2013

ISO 27001:2013 is a standard that defines the requirements for an Information Security Management System (ISMS), the set of policies, procedures and processes by which the management team of an organization manages Information Security effectively and efficiently. As such, it has a very broad scope, but it is limited in depth. Specifically, it defers to ISO 27002:2013 for actual controls.

The controls in ISO 27001:2013 consist of a set of declarative statements about what an organization has to do in order to be compliant. For instance, *Section 7 (Support), Subsection 5 (Documented information), subsubsection 2 (Creating and updating) (7.5.2) sub a: When creating and updating documented information the organization shall ensure appropriate identification and description (e.g a title, date, author, or reference number*. These are structured in sections 4 through 10 (sections 0 through 3 serve an introductory function), with each section having multiple subsections, and some subsections having subsections of their own. These declarative statements can be seen as controls, and can be encoded as such:

- ID (section, subsection, possibly subsubsection)
- Section name
- Subsection name
- Text of the control

Because ISO 27001:2013 and ISO 27002:2013 were only available in PDF format, and this PDF format did not allow copying and pasting, an Optical Character Recognition (OCR) tool was used to record the text of the documents, which was then transferred to a spreadsheet for further processing.

The structure of ISO 27002 is explained in its section 4, which explains:

> This standard contains 14 security control clauses collectively containing a total of 35 main security categories and 114 controls.

These 14 security clauses are contained in clause 5 through 18. Each clause (for instance, clause 5 ”Information security policies”) has one or more main security categories (for instance 5.1 ”Management direction for information security”) which contain security controls. Each security category also has an objective, stating what the goal of the security control is. Controls, in turn, contain the following information and can therefore be encoded as such:

- ID (for instance 5.1.1)
- Title
- Control (what has to be done)
- Implementation guidance (specific instructions in order to implement this control)

- Other information (additional considerations or motivation, if applicable).

4.4.1.2 NIST 800-53 revision 4

NIST 800-53 revision 4 (titled ”Security and Privacy Controls for Federal Information Systems and Organizations”; NIST [51]) is a catalog of controls which is mandatory for US federal information systems. The control catalog of NIST SP 800-53 revision 4 consists of 240 controls in 18 families, each control often having several control enhancements. Controls also have a baseline indication, which serves as a starting point for determining which controls should be implemented for information systems with a Low, Moderate or High impacts. The control enhancements can also be seen as controls in their own right, as they have virtually the same content. Finally, each control also has a priority (from P0 to P3), to help organizations prioritize and sequence implementation). Each of the controls and control enhancements contains the following information, and can be encoded as such:

- ID (*e.g. for controls ”SI-14”, and for enhancements ”SI-14 (1)”*)
- Control family
- Control title
- The control text
- Supplemental guidance (optional)
- Priority (P0 to P3)
- Related NIST 800-53r4 controls

The contents of the NIST SP 800-53r4 controls were available in several formats, namely Excel, PDF and XML. As the format of the Excel document was not easily parse-able to the format required for the database, a Python script was written to parse the XML file into a format that could be read into the database.

4.4.1.3 CIS Controls

Note that this refers to CIS Controls version 6.1, released in 2016. Version 7.0 was released during the writing of this thesis

The CIS Controls are a set of 20 prioritized, actionable and highly focused cybersecurity controls put together by an international community of practitioners and institutions [12]. Each control is subdivided into sub-controls. Each control and sub-control contains the following information, and can be encoded as such:

- ID (*e.g. 15 for a main control, or 15.6 for a sub-control*)
- Control text
- (*for main controls:*) Title of the control

- (*for main controls:*) Explanation as to why this control is critical
- (*for main controls:*) Procedures and tools, which gives high-level implementation guidance.
- (*for main controls:*) A System Entity-Relation diagram that shows the components of implementation.
- (*for sub-controls:*) Family (*System*, *Network* or *Application*)
- (*for sub-controls:*) Whether this control is Foundational or Advanced. In some cases, it marks a control as Foundational and gives some additional pointers for making this an Advanced control.

4.4.2 Combining the standards into one

The controls in the standards above were encoded and captured in spreadsheet form, in order to facilitate analyzing ISAMs. The standards were then translated into one data format, and categorized according to several categorization strategies.

It has been considered to attempt to combine the standards into one super-standard, by eliminating duplicates, and tracing controls to one etymology. This is the approach taken by Johansson and Johnson [39], although they do not explain in detail how they went about doing this. This approach is further complicated by the differing scopes of the standards and the different meanings that are sometimes given to terms. Additionally, this approach makes it very hard to preserve the context in which controls appear (such as the overarching goals in the case of the CIS Controls), and focuses solely on the ”what” of the controls while removing the ”why.” Combining them into one data format while preserving the controls as-is was determined to be a better approach in the face of these considerations.

Table 4.1 outlines the standardized data format, and shows how the structure of the standards above is mapped to this data format. It also gives an example for each data type. The ”standardized” format has been selected to fit all of the information in the tables.

The reason for separating the text of the controls in a *short* control text and a *long* control text is that some standards (for instance ISO 27002:2013) have a Clause name, Control text, and Implementation guidance, and bunching these together would conflate the text of the controls with the guidance on how to implement them.

A choice has been made to duplicate some of the information in some of the fields (for instance, the CIS Control’s Control name is mapped to both Control Name and Original Category). This was deemed more desirable than suddenly having empty cells.

Table 4.1: Mapping of all standards to one data format

Standardized	**ISO 27001**	**ISO 27002**	**NIST 800-53**	**CIS Controls**
ID	ID *4.1*	ID *5.1.1*	ID *AC-1*	ID *1*
Control Name	Section Name *Understanding the organization and its context*	Clause name *Policies for information security*	Control title *Access control policy and procedures*	Control name *Inventory of Authorized and Unauthorized Devices*
Short Control Text	Section Name *Understanding the organization and its context*	Control Text *A set of policies (...) shall be defined (...)*	Control title *Access control policy and procedures*	Control description *Actively manage (...) all hardware devices*
Long Control Text	Control text *The organization shall determine (...) information security management system.*	Implementation guidance *At the highest level (...) training programme.*	Control text *The organization [d]evelops, documents, and disseminates (...) [a]n access control policy (...)*	Control description *Actively manage (...) all hardware devices*
Original Category	Chapter name *Context of the organization*	Clause name *Information security policies*	Control family *Access control*	Control name *Inventory of Authorized and Unauthorized Devices*

Figure 4.1: The functions and activities of the NIST CSF

Identify (ID)	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect (PR)	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect (DE)	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond (RS)	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover (RC)	Recovery Planning
	Improvements
	Communications

4.4.3 Categorization of controls

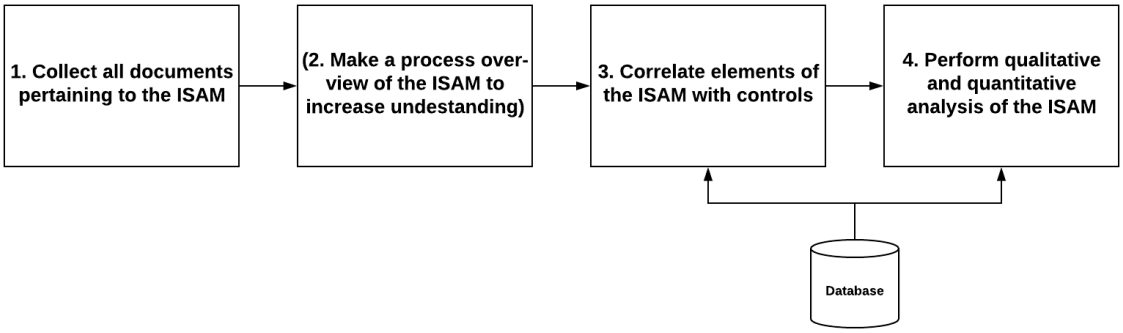
In order to properly measure the degree to which various areas of Information Security are covered by an ISAM, it is important to categorize the controls appropriately. One such categorization can be found in Johansson and Johnson [40], where they made a database of controls based on several information security standards and categorized each control along the dimensions of *scope*, *purpose* and *time*. However, it was found that categorizing the controls along this way would be arbitrary. A decision was made to use the NIST CSF, because it was determined to be a good umbrella framework to fit other controls under. It also encompasses the *scope* dimension used by Johansson and Johnson [40].

The NIST CSF [52] is a cybersecurity framework developed by the US government, and consists of a *core*, *implementation tiers* and a *profile*. The latter two are implementation-focused guidelines on how to apply the CSF in an organization. The core consists of five core *functions*, which are each subdivided into *activities*, in turn subdivided into specific *subcategories*, which each have informative references that map them to several industry standards, including the ISO 27001:2013 set of standards, the CIS Controls, and NIST SP 800-53r4.

The functions and the activities that they are subdivided in are outlined in Figure 4.1

The informative references also enabled the ISO 27001:2013, NIST CSF and CIS Controls to be mapped to the CSF. The ISO 27002:2013 controls were mapped to the NIST SP 800-53r4 controls through Appendix H of the NIST SP 800-53r4,

Figure 4.2: Structure of the framework



which in turn enabled the ISO 27002:2013 controls to also be mapped to the CSF.

4.5 Applying the framework

This section outlines the process by which the framework is applied, which is also outlined in figure 4.2. First, this section outlines the required inputs for the process, which are usually in the form of unstructured text. Then, it outlines the steps taken, and explains each step, along with considerations and pitfalls. Finally, the section outlines the outputs of this section.

4.5.1 Input requirements

The aim of this framework is to measure ISAM. To that end, the input required is the material supporting an ISAM. Specifically, the input needs to meet the following criteria:

- **Concrete.** Valid input needs to be in written form, for instance in the form of checklists, spreadsheets, or some other form of documents.
- **Structured.** Valid input needs to be structured in a logical and consistent manner. It is hard to map unstructured content to controls.
- **Specific.** The ISAM needs to be specific and unambiguous about what it measures, and for what purpose it is measured if the context of the question does not explain it.

4.5.2 Process steps

This section outlines the steps taken while analyzing an ISAM, and explains the rationale behind each step. First the steps are listed, and then each step is explained in more detail.

The steps that are taken in analyzing an ISAM are as follows:

- Collect all documents, materials and other information relevant to the ISAM
- (Optional) Make a process overview of the ISAM in order to increase understanding and completeness
- For each document, material and other piece of information pertaining to the ISAM: attempt to correlate all elements to the controls that they cover.
- Roll-up: report on the completeness and quality of the ISAM.

4.5.2.1 Document collection

The aim of this step is to ensure that all of the information regarding the ISAM is available. The researcher asks one or more stakeholders to gather all documents pertaining to the ISAM, including documentation, guidelines and handbooks for applying the ISAM. Then, the researcher reads through the documents and makes an initial judgment on whether this documentation is sufficient for a researcher to perform the ISAM.

Since the consultants likely possess at least some knowledge that is tacit (i.e. un-codified, informal, implicit or uncaptured information), the researcher should take this into account and ensure that he understands the context in which the ISAM is performed. At the very least, this tacit knowledge may have to do with where documentation or additional knowledge can be found. Tacit knowledge may also include knowledge that is expected of consultants, either from experience or from certifications, like for instance an ISO 27001:2013 certified consultant.

If there are multiple documents, it may be useful to catalog the documents that make up the ISAM. The goal here is to ensure that each element of the ISAM can be uniquely identified.

The result of this step is a cataloged set of documents. Each of the documents, and each of the parts of this document, should be addressable in a uniform way. This means that every element in the ISAM should be uniquely identifiable.

4.5.2.2 Process overview

In order to get a more complete overview of an ISAM, diagrams such as an UML Activity Diagram or a flowchart can help to analyze the ISAM, and verify that all of the documents that are being used are also identified in the previous step. Conversely, this step may also identify documents that are not necessary to the process.

In analyzing the State of Security assessment, for instance, a flowchart was created of the process that was followed, and the sequencing of events and actors in this process (see figure 5.1), and this was used in order to validate with the stakeholders that all of the events and documents were captured.

It should be noted that this step is optional. If the process of the ISAM is trivial, there is no need to create additional insight into the process.

4.5.2.3 Correlate elements to controls

The database of controls that was created in chapter 4 is used in this chapter to correlate all of the elements in the ISAM to controls in the various standards. To this end, all of the individual elements (checklist items, questions, and other methods of eliciting information from the organization, should be traced to specific controls. This requires the researcher to have knowledge of the content of all of the controls in the database.

For each of the elements in the ISAM, follow the following process:

- Find all of the controls in the database that the element corresponds with.
- For each of these controls, write down the ID of the control, and the degree to which the element measures the control. Choose from 0 (not at all), 1 (somewhat/partially), 2 (mostly) and 3 (completely).
- Finally, for each of the controls that none of the elements of the ISAM get mapped to, go through the ISAM and ensure that none of the elements map to this control. If there are none, mark the control as a 0.

The output of this step serves as the input for the following step.

4.5.2.4 Analyze and report

The results of the previous step are automatically parsed in a set of graphs that visually display how well the standards are covered by the ISAM. An analysis of these graphs gives insight into how well each of the standards is covered.

In order to analyze an ISAM, the researcher records the degree to which each control is measured by the ISAM on a scale of zero to three. These controls are analyzed by automatically counting how many controls got scored 0, 1, 2 and 3 for each standard. These are subdivided into the different control categories for these standards. These counts are then transformed into graphs (such as figure 5.5).

The graphs are stacked bar charts. The height of the bar chart corresponds to the number of controls that the corresponding section, subsection, chapter or category consists of. From bottom to top, the bar chart shows the number of controls that are covered completely (3), mostly (2), partially/somewhat (1), or not at all (0).

Finally, an interpretative step is needed. In this step, go through each graph and comment on the degree to which the section is measured. If a section is poorly measured, determine the impact that this has on the overall quality of the ISAM.

4.6 Conclusion

In this chapter, the process by which the framework was developed was outlined, and design choices are justified. It outlines the requirements for the framework, and the process is outlined by which the standards were selected that went into the framework. Finally, the input requirements for an ISAM for applying the framework were outlined, and the process is outlined by which the framework is applied.

The *Document gathering* step consisted of asking for the State of Security assessment worksheet, which was the only working document in the State of Security assessment. This step was not documented

Chapter 5

Case Study

The goal of this thesis is to develop a framework for validating ISAMs. In order to verify whether the OSSUM framework is suited for this task, it is applied to an ISAM developed by Dutch Information Security organization Northwave, which is called the *State of Security assessment*. This chapter first explains the State of Security assessment in some detail. It then goes on to outline the goals of the case study, and how the case study achieves these goals. Finally, it explains the results of the case study.

5.1 The State of Security assessment

The State of Security assessment is an ISAM developed by Northwave, and aimed at analyzing the level of Information Security within an organization, focusing on the organizational, technical and behavioral aspects of Information Security. Considering the fact that privacy has become a very important area of Information Security lately, the State of Security assessment also checks whether the organization adheres to the GDPR [20].

It is based on several Information Security standards and frameworks, including the ISO 27001 family of standards and the CIS Controls, as well as relevant privacy laws (mainly the GDPR), prior experience in conducting Information Security assessments, and lessons learned through applying the State of Security assessment in previous iterations.

5.1.1 Overview of the process

Note: a new version of the State of Security assessment was developed during the writing of this master thesis. This section presents the version that the case study is based on.

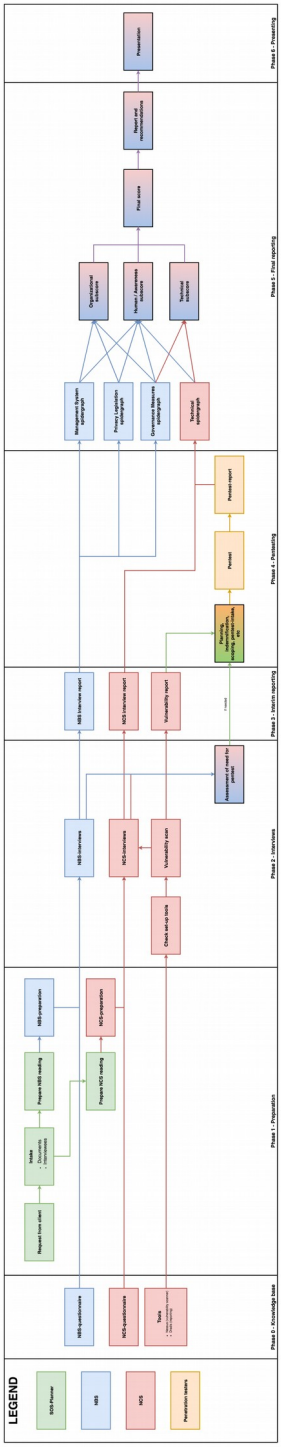


Figure 5.1: Flowchart of the SOS Process

The State of Security assessment (see figure 5.1) starts with a sales and intake procedure. During this procedure, Northwave asks for documentation that is relevant for determining how the organization deals with Information Security and how they have implemented it. Northwave also asks for a list of interviewees, which includes at least the CEO, systems administrator and CFO. Finally, some information is also requested, for the purpose of the vulnerability scan and the **pentest!** (**pentest!**).

The sales team prepares relevant documentation for the Northwave Business Security (NBS) and Northwave Cyber Security (NCS) consultants, who perform some desk research prior to the interviews on location. Using the documentation available, they formulate answers to some questions in the questionnaire in advance.

An interview is conducted on location by an NCS and an NBS consultant. During this interview, the consultants ask each of the stakeholders questions from the questionnaire, which pertain to the different clauses of the ISO 27001:2013 and ISO 27002:2013 standards, as well as questions which are based on the CIS Controls.

During the interviews, the NCS consultant performs a vulnerability scan of the organization's internal network using a laptop with the Nessus vulnerability scanner. This vulnerability scan also provides some input during the interview.

After the interview, the consultants decide together with the organization whether a pentest (short for penetration test) is required, and what the scoping of the pentest will be. The pentest will later be done remotely, and will often involve a customer website or customer portal.

The NCS and NBS consultants then write a preliminary report based on the interview, and an automated report is generated based on the vulnerability scan. The report for the vulnerability scan also serves as input to the pentest.

After the pentest has been planned, an Offensive Security Certified Hacker (OSCP) certified ethical hacker will attempt to compromise the application or website. All vulnerabilities that are found are documented in a pentest report.

In the final phase, all of the findings are combined into several spidergraphs, which indicate the level of maturity on how they manage their ISMS and the governance controls the organization has put into place, their compliance to relevant privacy laws, and the degree to which their IT infrastructure is resistant to internal and external threats. These spidergraphs are then transformed into an organizational subscore, a behavioural subscore (comprising of knowledge, attitude and awareness), and a technical subscore. Finally, these subscores are used to calculate a final grade for how mature the organization's is in terms of Information Security.

Northwave then presents the findings to the organization, and delivers a report with recommendations on how to improve the level of Information Security. The result of a State of Security assessment is therefore a clear plan with actionable advice to improve the level of Information Security within the organization.

5.2 Goal of the case study

The overall goal of this thesis is to validate ISAMs based on relevant Information Security frameworks and standards. This case study serves as the validation of the framework. The case study documents the application of the framework to the State of Security assessment.

The goal of the case study is therefore to demonstrate that the framework can be used in practice to validate an ISAM.

Note: there is not a lot of content here. May merge it with another section.

5.3 Results of the case study

In this section, the results of the case study are outlined. First, some additional insight is generated on the standards that make up the OSSUM framework. Then, an in-depth analysis is given of the SOS, and how well it adheres to each of the standards that are in the framework.

5.3.1 Performing the case study

This section outlines how the case study is actually performed, and the steps that have been taken.

First, an analysis was conducted of the State of Security assessment. This analysis consisted of interviews with stakeholders, desk research into the standards that make up the State of Security assessment and the documents used in administering the State of Security assessment to customers, and hands-on experience administering the State of Security assessment at a customer organization. This resulted in the flowchart depicted in 5.1.

The documents that are used in performing a State of Security assessment were gathered and analyzed. The main document consisted of an Excel worksheet, with questions structured along the categorization of the ISO 27001:2013 and ISO 27002:2013 standards, and questions that were inspired by the CIS Controls.

In analyzing the worksheet, the questions in the worksheet were traced to individual controls in the several standards that make up the database. For each, a determination was made of how well the question tests adherence to the control.

Figure 5.2 shows a small selection of ISO 27001:2013 controls, and the way they were analyzed in the case study. The first three columns indicate the control, and the colored column indicates how well the column is measured, and if so by which control. This serves as an illustration of how the OSSUM framework is used.

Figure 5.2: Small selection of controls as measured by the State of Security assessment

	A	B	C	CA	CB	CC	CD
1	Sta	Sta	ID	CS:SOS-control - 1	CS:SOS-control	CS:judgment	CS:remarks
2	ISO	ISO	4.1	27001	4.1	2	
3	ISO	ISO	4.2	27001	4.2	2	
4	ISO	ISO	4.3	27001	4.3	0	The question cited asks about risks, not scope.
5	ISO	ISO	4.4	27001	4.4	2	Question does ask about it, but not implementation details
6	ISO	ISO	5.1	27001	5.1	1	Questions don't ask, for instance, about resources and continual improvement
7	ISO	ISO	5.2	27001	5.2	3	
8	ISO	ISO	5.3	27001	5.3	3	
9	ISO	ISO	6.1.1	27001	6.1.1	0	No evidence yet
10	ISO	ISO	6.1.2	27001	6.1.2	2	Questions ask about risk assessment
11	ISO	ISO	6.1.3	27001	6.1.3	2	Questions ask about what the infosec risk treatment process looks like
12	ISO	ISO	6.2	27001	6.2	3	This is adequately asked
13	ISO	ISO	7.1	27001	7.1	3	Is being asked
14	ISO	ISO	7.2	27001	7.2	3	

In the end, a numerical analysis of the State of Security assessment is performed. The database automatically calculates how many controls for each standard have been determined to be measured, and to which degree. A part of the numerical analysis is shown in figure 5.3. This part shows the number of controls in each of the chapters, divided over each of the levels defined in table 5.1.

The numerical analysis is used to generate graphs such as the one displayed in 5.5. These graphs serve as the starting point for writing an analysis, as they provide a highlevel overview of the coverage of each standard. Recommendations are made to increase the coverage of the individual standards, where applicable.

Additionally, the categories of the NIST CSF are taken to represent a highlevel overview of the different aspects of Information Security, and recommendation are made to improve the coverage of categories within the NIST CSF, in order to increase the Information Security coverage of the State of Security assessment as a whole.

Figure 5.3: Statistical analysis of the State of Security assessment in the case study

1	Categoryname	Sub	Sub	Label	3	2	1	0	Tc	% 3	% 2	% 1	% 0
2	Context of the organization	-	-	4 - Context of the organizat	0	3	0	1	4	0,00%	75,00%	75,00%	100,00%
3	Leadership	-	-	5 - Leadership	2	0	1	0	3	66,67%	66,67%	100,00%	100,00%
4	Planning	-	-	6 - Planning	1	2	0	1	4	25,00%	75,00%	75,00%	100,00%
5	Support	-	-	7 - Support	2	4	1	0	7	28,57%	85,71%	100,00%	100,00%
6	Operation	-	-	8 - Operation	3	0	0	0	3	100,00%	100,00%	100,00%	100,00%
7	Performance evaluation	-	-	9 - Performance evaluation	0	2	1	0	3	0,00%	66,67%	100,00%	100,00%
8	Improvement	-	-	10 - Improvement	0	2	0	0	2	0,00%	100,00%	100,00%	100,00%

Table 5.1: Legend - degree to which a control is measured by an ISAM

Level	Description	Explanation
0	Not at all	This control is not measured at all by the ISAM
1	Somewhat/partial	This control is not measured in detail, or only partially, by the ISAM
2	Mostly	This control is mostly measured by the ISAM
3	Completely	This control is completely measured by the ISAM

5.3.2 Overview of adherence to standards

This section analyzes how well the OSSUM framework tests an organization's adherence to the standards under consideration in a statistical method. It will contain an overall statistical analysis of the State of Security assessment, as well as an interpretation of that analysis.

As outlined in section 5.3.1, each of the questions in the State of Security assessment has been traced to the corresponding controls in the various standards, and an assessment was made on how well the question measures the control. These assessments were graded on a scale of zero to three, as demonstrated in table 5.1. This section gives some insight in how well each standard is covered by looking at the number of controls that are covered by the State of Security assessment. Graphs were generated for this purpose.

5.3.2.1 ISO 27001:2013

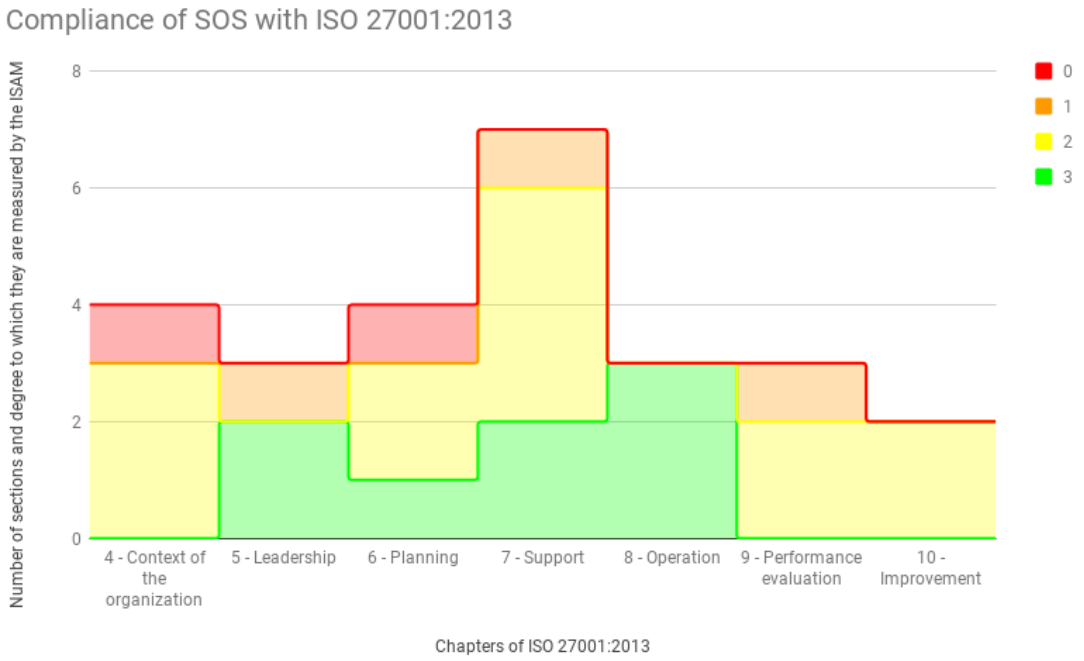
Figure 5.4 shows each of the clauses in the ISO 27001:2013 standard. For each of the clauses, it shows how many of the controls are measured by the State of Security assessment, and to what degree.

Unlike the ISO 27002:2013 clauses, the ISO 27001:2013 clauses were not categorized further than their individual controls.

It should be noted that this measurement serves only as an indicator of the quality of the questions in the questionnaire, since the consultants are required to have demonstrable experience with ISO 27001:2013.

Each of the clauses in the ISO 27001:2013 standard are measured to at least some degree, with each clause having at least two sections that are measured to a

Figure 5.4: Highlevel overview of coverage of ISO 27001:2013 by State of Security assessment



great degree.

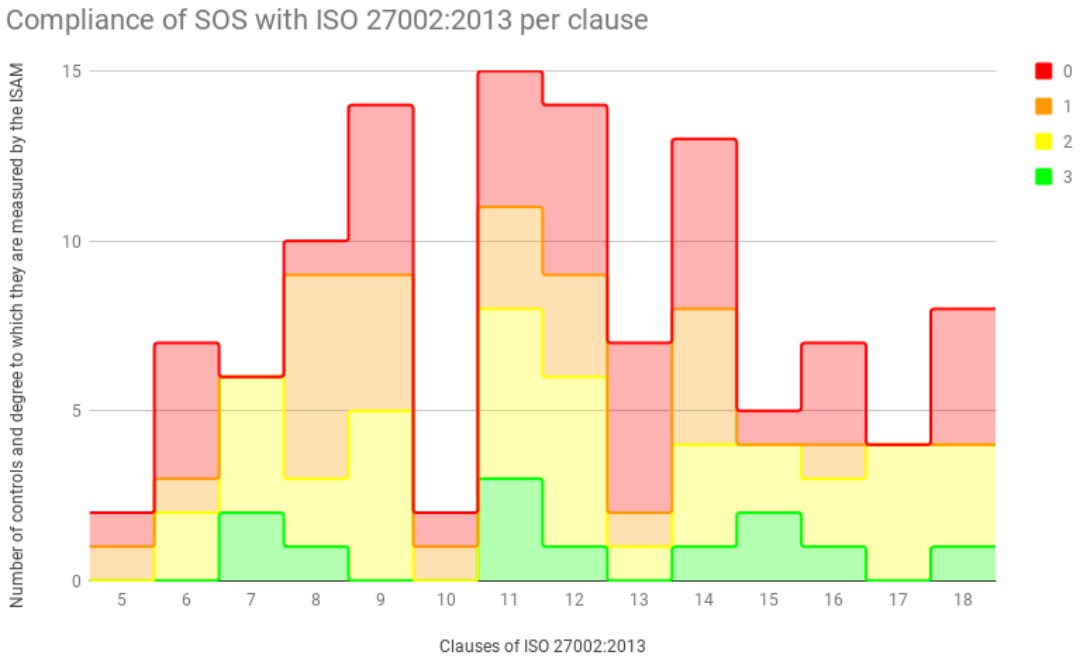
Noteworthy is that clauses 4 (*Context of the organization*), 9 (*Performance evaluation*) and 10 (*Improvement*) have no sections that were judged to be measured completely.

5.3.2.2 ISO 27002:2013

Figure 5.5 shows to what degree each of the clauses of the ISO 27002:2013 standard is covered by the State of Security assessment. These clauses are further split down into control categories in figure 5.6. It should be noted here that the graphs also show the absolute number of controls in each of the clauses and categories. Table TODO MAKE TABLE shows the structure of the ISO 27002:2013 standard, and can be used as a legend for these figures.

What immediately jumps out is that clause 5 (*Information Security Policies*) and clause 10 (*Cryptography*) do not appear to be very well covered by the State of Security assessment at first glance. An explanation for why they have so few controls that are either completely (*3*) or mostly (*2*) measured, is because these clauses contain a relatively low number of controls to begin with (2 each). Clause 13 (*Communications Security*) also contains a relatively large number of sections that are not measured, with only one of its seven controls being mostly measured. The other

Figure 5.5: Highlevel overview of coverage of ISO 27002:2013 by State of Security assessment

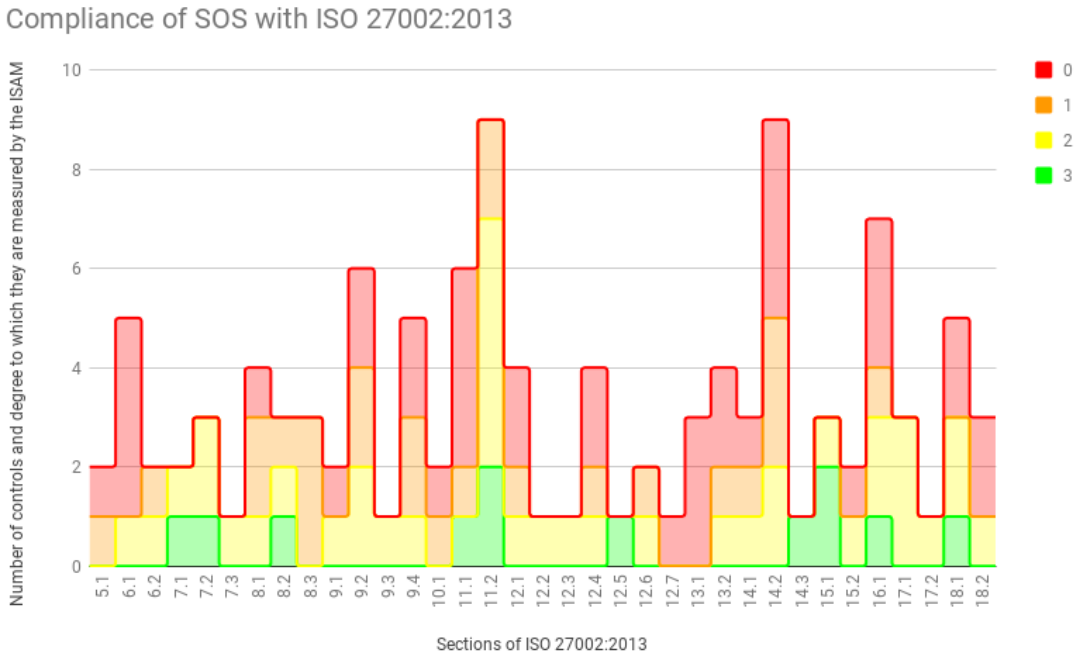


controls have at least 2 controls that are mostly measured by the State of Security assessment. What this means is that, apart from the clauses mentioned above, the State of Security assessment appears to have a balanced selection of controls from the ISO 27002:2013 standard.

This is also reflected when this is broken down into the individual control categories that make up the ISO 27002:2013. Out of the 35 control categories, there are two that do not contain a control that is measured (level 0; category *12.7 Information Systems audit considerations* and category *13.1 Network Security Management*), with two more control categories that have at most a control that is only partially measured (level 1; category *5.1 Information Security policies - Management directions for Information Security* and category *10.1 Cryptography - Cryptographic controls*).

Furthermore, out of the five controls that make up category 6.1 (*Organization of information security - Internal Organization*), only one was determined to be level 2 (*mostly measured*), and out of the three controls that make up category 18.2 (*Information Security reviews*), likewise only one was determined to be level 2 (*mostly measured*). Finally, while all three of the controls that make up category 8.3 (*Asset Management*) were determined to somewhat measure the control (*level 1*), none of the controls are determined to be mostly measured by the State of Security assessment.

Figure 5.6: Detailed overview of coverage of ISO 27002:2013 per control category



Finally, it should be noted that the above analysis is performed over the questions in the questionnaire that is to be used during the interview, which is conducted by an ISO 27001:2013 certified Information Security consultant, and that the questions are meant to be used as a fallback for the interviewer rather than a fully structured guideline. This means that Northwave should make a determination which recommendations to follow.

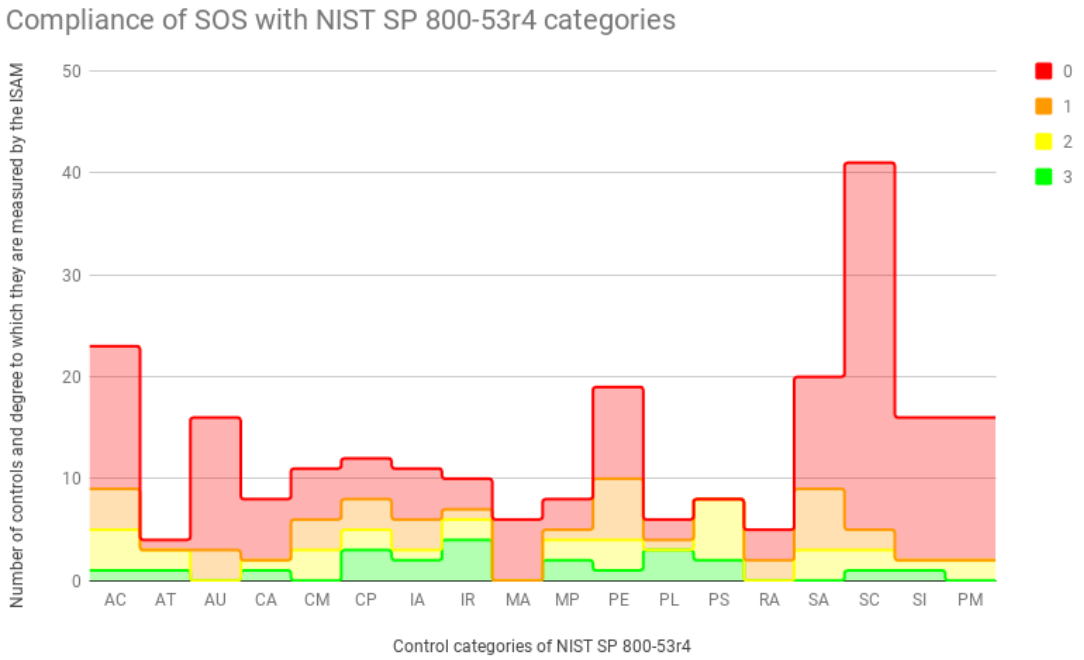
5.3.2.3 NIST SP 800-53r4

While the NIST SP 800-53r4 is a catalog of cybersecurity controls that is primarily aimed at federal organizations in the United States of America, it can also be applied to organizations outside the federal government of the United States of America. Figure 5.7 shows how well the control categories in the NIST SP 800-53r4 are measured by the State of Security assessment.

It is important to note that implementing NIST SP 800-53r4 does not mean that every control in the catalog has to be implemented by the organization. Rather, as with ISO 27002:2013, a selection of the controls will have to be made based on a risk assessment.

Of note is that the NIST SP 800-53r4 appears to be much less well-covered than the ISO 27001:2013 and ISO 27002:2013 standards, with a relatively large number of controls that are not measured by the State of Security assessment (level *0*.

Figure 5.7: Highlevel overview of coverage of NIST SP 800-53r4 by State of Security assessment



Nevertheless, most categories do have some amount of controls that are measured completely (level *3*) or mostly (level *2*). An explanation for why a relatively large number of NIST SP 800-53r4 controls are not measured can be found in the fact that many of the controls and subcontrols of the NIST SP 800-53r4 go beyond what is required for the purposes of a State of Security assessment.

Specifically noteworthy is that none of the controls in the NIST SP 800-53r4 category *Maintenance* are measured.

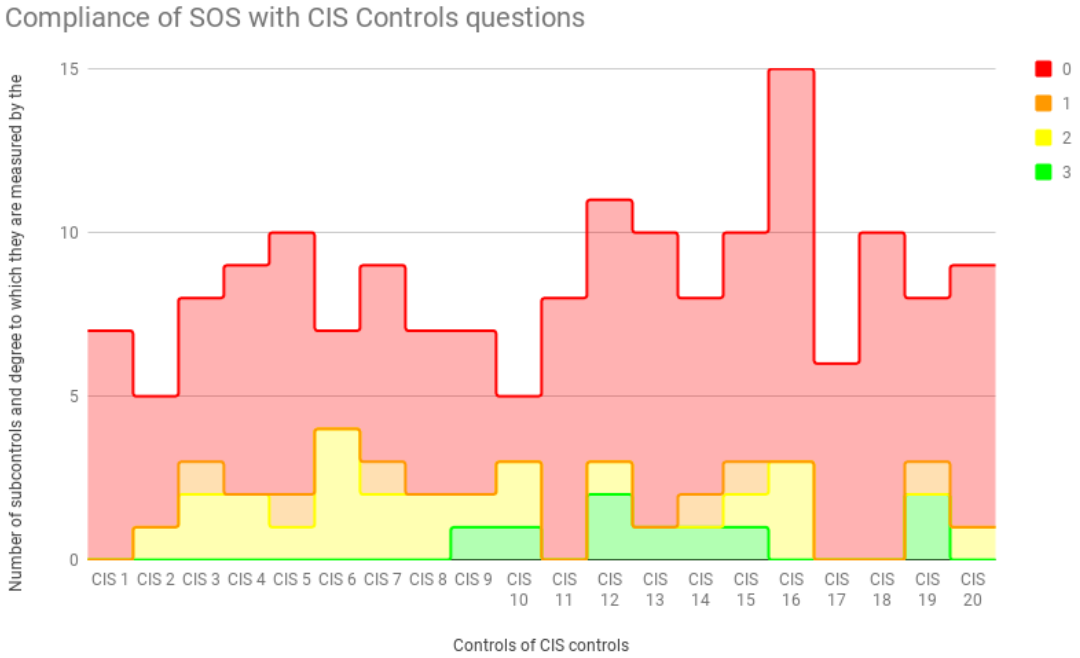
Additionally, none of the controls in both the NIST SP 800-53r4 Families *Auditing and review* and *Risk assessment* have no controls which were determined to mostly be measured by the State of Security assessment.

Finally, a relatively large number of the controls in the *System and Communication* family are not measured by the State of Security assessment (level *0*). This may be explained by the fact that the State of Security assessment is designed around ISO 27001:2013, and in part because the NIST SP 800-53r4 is not designed to be universal in nature, but rather is aimed at federal organizations.

5.3.2.4 CIS Controls

The CIS Controls are a prioritized, industry-driven set of cybersecurity standards that are aimed at improving organizations' cybersecurity posture. They are devel-

Figure 5.8: Overview of coverage of CIS Controls by State of Security assessment



oped by the SANS institute. They are a best-practice standard that is widely used by organizations.

Figure 5.8 shows the coverage of the CIS Controls by the State of Security assessment. The questions in the State of Security interview document were traced to the subcontrols that make up these controls.

There are several CIS Controls that could not be traced to questions in the State of Security assessment, namely 1 (*Inventory of Authorized and Unauthorized Devices*), 11 (*Secure Configurations for Network Devices*), 17 (*Security Skills Assessment and Appropriate Training to Fill Gaps*) and 18 (*Application Software Security*). Furthermore, control 2 (*Inventory of Authorized and Unauthorized Software*) and control 20 (*Penetration Tests and Red Team Exercises*) have only one subcontrol that is mostly measured by the State of Security assessment, and other subcontrols are not measured.

Apart from these parts, the State of Security assessment appears to measure a balanced number of subcontrols from each CIS Controls.

An explanation for why the CIS Controls appear to be measured only to a modest degree may be that the subcontrols are very specific, while the questions in the State of Security assessment questionnaire are mostly highlevel and rely on the interviewer to ask deeper questions when necessary.

5.3.3 Improvement recommendations

This section recommends potential points of improvement for the State of Security assessment. TODO: add numbering to recommendations.

5.3.3.1 Compliance with ISO standards

Overall, the compliance with ISO standards is good, and most of the ISO controls that were determined to be not or mostly not measured by the State of Security assessment either had to do with questions specific to an ISMS. As the goal of the State of Security assessment is not to measure an organization's SMS, but rather its Information Security posture, these questions are less relevant.

One of the more relevant omissions is ISO 27001:2013 control category 6.1, *Actions to address risks and opportunities - General*, as there is no formal risk assessment in the State of Security assessment. This is also not covered by any of the other standards.

> Recommendation 1: Consider adding a risk assessment to the State of Security assessment.

The State of Security assessment questionnaire does not ask extensively about how the organization manages an asset and software inventory, as required by ISO 27002:2013, clause 8 (*Asset management*). While the vulnerability scan does give Northwave some insight in which assets there are, and the network overview and Configuration Management Database (CMDB) requested at intake may provide some insight, concrete questions about how the organization manages their hardware and software.

> Recommendation 2: Include questions on how the organization manages an asset inventory and software inventory, and how the organization performs asset management, if not already adequately covered by the desk research.

While the consultants can get a reasonable feel for how well an organization manages their physical security, the State of Security assessment does not ask a lot of questions about physical security. Northwave will have to determine whether the level of insight consultants get is sufficient in determining whether or not to adopt this recommendation.

> Recommendation 3: Include questions about physical security into the State of Security assessment, including questions regarding the implementation about security areas and the physical security of the server room.

Overall, the coverage of the ISO 27001:2013 standards by the State of Security assessment questionnaire is comprehensive. Barring minor exceptions, omissions are overall explained by the goal of the State of Security assessment, namely to deliver an expert opinion on the level of Information Security (rather than performing an in-depth audit).

5.3.3.2 NIST SP 800-53r4

Many of the NIST SP 800-53r4 controls that are not covered by the State of Security assessment are very detailed, and are beyond the level of detail that is required for the purposes of a State of Security assessment. Therefore, the recommendations below should not be regarded as essential omissions, but rather as potential points for deepening the State of Security assessment.

In general, the *Access Control* and *Awareness and Training* families of controls are reasonably covered for the purposes of the State of Security assessment. The *Audit and Accountability* family of controls, however, could be covered better by adding questions to the State of Security assessment about how the organization ensures actions by employees can be audited and can be accounted for. Controls AU-1, which states that the organization should have an audit and accountability policy, and AU-2, which states among other things that the organization needs to have thought about which events need to be auditable, may be beneficial. Northwave will need to make a determination whether it is necessary for the purposes of the State of Security assessment to ask about controls regarding audit and accountability.

> Recommendation 4: Determine whether to add more questions to the State of Security assessment about auditing and accountability.

The *Maintenance* family of controls of the NIST SP 800-53r4 is not measured by the State of Security assessment. These NIST SP 800-53r4 controls mostly pertain to ensuring the authentication, authorization and accountability of maintenance, and making sure maintenance is properly authorized. While NIST SP 800-53r4 considers Maintenance important enough to warrant its own family of controls, it should be noted that NIST SP 800-53r4 is aimed at organizations in the federal US government, and organizations taking a State of Security assessment are usually smaller in scope. Northwave should make a determination whether measuring the authentication, authorization and accountability of maintenance falls within the scope of the State of Security assessment. These controls are also not measured in significant detail elsewhere in the State of Security assessment.

> Recommendation 5: Determine whether to add questions to the State of Security assessment that pertain to scheduled and unscheduled maintenance.

Finally, the *Risk assessment* family of controls is not extensively measured by the State of Security assessment in its current state, as was noted in recommendation 1.

5.3.3.3 CIS Controls

Most of the CIS Controls are well covered by the State of Security assessment. This section outlines potential points of improvement in the State of Security assessment based on the CIS Controls.

CIS Controls 1 (*Inventory of Authorized and Unauthorized Devices*) and 2 (*Inventory of Authorized and Unauthorized Software*) are not measured very well by the State of Security assessment. These are among the first five CIS Controls, which SANS refers to as providing cybersecurity ”hygiene.” SANS claims that ”implementation of the first five controls provides an effective defense against the most common cyber-attacks (80% of attacks)” [13]. This has already been addressed in recommendation 3.

CIS Controls 11 (*Secure Configurations for Network Devices*) is also not very well measured by the State of Security assessment. This control mostly measures whether routers, switches and access points are configured in a secure manner. This may be too specific for the State of Security assessment, and depending on the scope of the State of Security assessment this may not be relevant.

> Recommendation 6: Determine whether to add questions regarding the secure configuration of network devices, as mentioned in CIS Controls 11.

CIS Controls 17 (*Security Skills Assessment and Appropriate Training to Fill Gaps*) is not measured very well, either. This control mostly measures security awareness and training of employees. Because of the prevalence of social engineering and other attacks that seek to target employees, it is recommended that the State of Security assessment measures awareness and knowledge of Information Security.

> Recommendation 7: Add questions to the State of Security assessment to measure how the organization ensures that employees have adequate knowledge to recognize Information Security incidents, and respond to them appropriately.

Finally, CIS Controls 18 (*Application Software Security*) is not measured very well by the State of Security assessment. This control mostly measures how well the organization secures applications that are developed by the organization itself,

and how well the organization ensures that third party applications are supported and updated. This is also not covered elsewhere by the State of Security assessment. Depending on the scope of the State of Security assessment, a determination should be made whether adding questions about Application Software Security is necessary.

> Recommendation 8: Determine whether to add questions to the State of Security assessment to measure the implementation of security measures for applications that are developed in house, as well as third party applications.

5.3.3.4 NIST Cybersecurity Framework

The NIST CSF is a framework that can be used as an ”umbrella” for the other standards that were used to develop the OSSUM framework described in this thesis. It can be used to distinguish between the various aspects of Information Security, and can be used to determine the degree to which all aspects of Information Security are covered by an ISAM. During this thesis, all of the controls in the other standards were mapped to the NIST CSF. The analysis of how well the different categories of the NIST CSF are covered by the State of Security assessment.

Figure 5.9 shows the different Activities of the NIST CSF, and the degree to which they are covered by the State of Security assessment. Figure 4.1 outlines the five core Functions of the NIST CSF, and the Activities that make up those Functions. What should be noted is that there is a large difference between the number of controls that measure each Activity, as can be seen by comparing the absolute height of the different bars in figure 5.10. The Activity *Protect - Information Protection Processes and Procedures (PR.IP)*, for instance, is measured by 119 controls spread over all standards, while *Identify - Risk Management Strategy (ID.RM)* is only measured by 4 controls spread over all standards, and *Protect - Maintenance (PR.MA)* is measured by 7 controls over all standards. This may be because Activities that are considered may be measured to a more detailed degree than Activities that are considered less important.

While the State of Security assessment measures most of the Activities to a reasonably high degree (with most of the Activities being mostly measured (*level 2*) by at least 30% to 50% of existing controls), *Identify - Risk Management Strategy (ID.RM)* and *Protect - Maintenance (PR.MA)* are measured to a lesser degree. None of the 4 controls that make up ID.RM are measured by the questionnaire used in the State of Security assessment, and of the 7 controls that make up ID.RM two are mostly measured (*level 2*), and the rest is also not measured at all. A determination should be made by Northwave whether this is acceptable.

> Recommendation 9: Determine whether the State of Security assessment should measure Risk Management Strategy and Maintenance to a more detailed degree.

Identify - Risk Assessment (ID.RA) is another Activity that is not very well measured. Of the 31 controls that make up this Activity, 3 are completely measured (*level 3*) and 2 are mostly measured (*level 2*), but 20 are not measured at all (*level 0*). Considering the important role that Risk Assessment plays in Information Security, Northwave may want to consider improving the coverage by the State of Security assessment of this area.

> Recommendation 10: Add more questions regarding Risk Assessment to the State of Security assessment in order to increase the coverage of the *ID.RA* Activity.

Finally, 5.9 shows how many controls measure each of the core Functions of the NIST CSF. While this overview is most likely not granular enough to elicit useful recommendations, it is interesting to see that the Protect Function has the largest number of controls by a wide margin. This indicates that, in general, Information Security standards put an emphasis on protecting assets from harm.

In general, barring the recommendations made in this section, the State of Security assessment covers the various aspects of Information Security rather well.

5.4 Conclusion

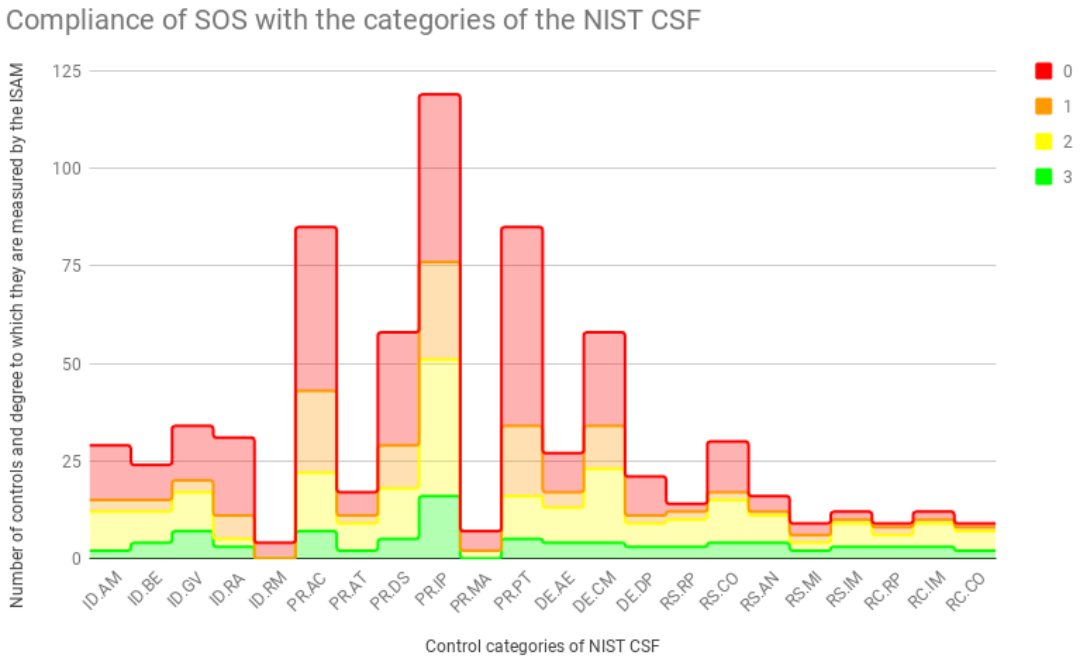
In this case study, the State of Security assessment was analyzed alongside the standards that were adopted in the OSSUM framework. The case study analyzed how well each of the standards is covered by the State of Security assessment. It gave an overview of how well each of the categories and subcategories are covered by the State of Security assessment. Finally, this case study gave recommendations on how to improve the State of Security assessment, and in doing so demonstrated the suitability of the OSSUM framework.

The document collection step, which is outlined in section 4.5.2.1, was rather brief in the case of the State of Security assessment, since the entire set of documents consisted of one worksheet, and was not documented due to its brevity.

The *Process overview* step, which is outlined in section 4.5.2.2, consisted of creating a flowchart of the State of Security assessment. This flowchart is shown in 5.1.

The *Correlate elements to controls* step, which is outlined in section 4.5.2.3, is documented in section 5.3.1.

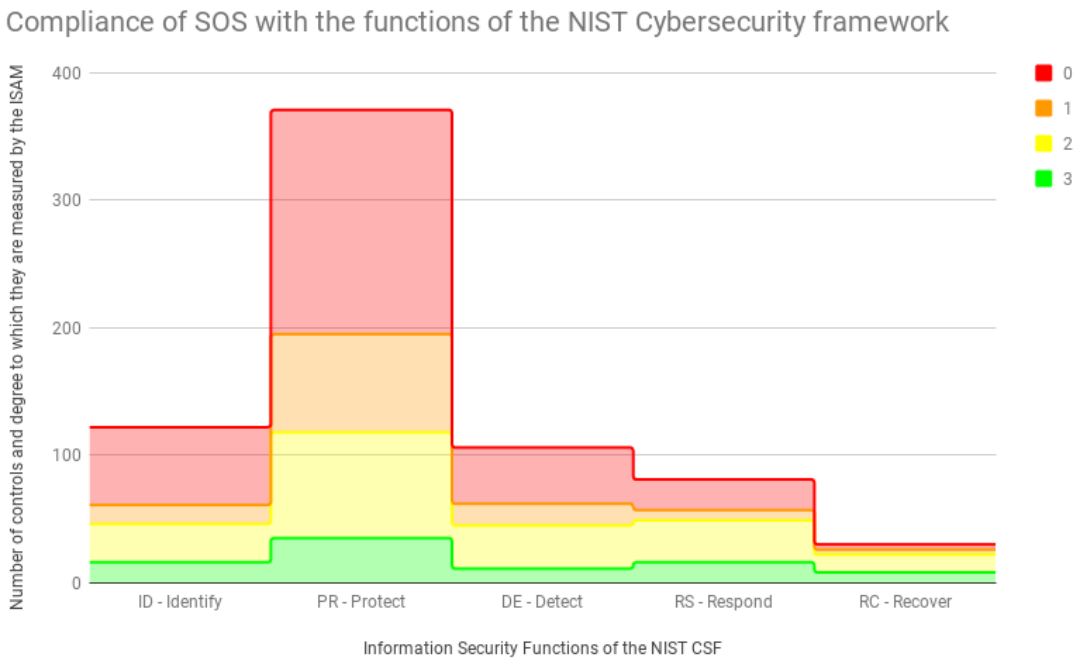
Figure 5.9: Detailed overview of coverage of the Activities in the NIST CSF by State of Security assessment



Finally, the *Analyze and report* step, which is documented in section 4.5.2.4, is documented in section 5.3.3. This section discusses the results in section 5.3.1, and makes recommendations based on the results of the previous step.

Based on the results of the case study, the State of Security assessment covers relevant Information Security standards well. No major omissions could be found, and several recommendations were made in order to improve the coverage of relevant standards by the State of Security assessment.

Figure 5.10: High-level overview of coverage of the Functions in the NIST CSF by State of Security assessment



Chapter 6

Conclusions and future work

6.1 Conclusions

Subquestion 1, "*Which standards, guidelines and other relevant materials should be covered by an information security assessment methodology?*" is answered by chapter 2, which gives background information on the most relevant Information Security standards found in the literature study.

In answering subquestion 1.1, "*In which ways can the controls found in these standards be categorized?*" several methods of categorizing controls have been considered. Apart from categorizing the controls using the categories given in the standards themselves, the controls were mapped to the NIST Cybersecurity Framework (CSF). These categories proved useful when eliciting recommendations.

Subquestion 2, "*How can Information Security Assessment Methodologies be validated according to relevant Information Security standards?*" was answered by designing the framework that is described in this thesis. The design of the OSSUM framework is presented in chapter 4. This design builds on the categorization of controls which was investigated in answering subquestion 1.1, and relies on it for analyzing ISAMs. Additionally, this thesis presents a case study in which the OSSUM framework is used for analyzing the coverage of relevant Information Security standards of an ISAM known as the State of Security assessment, and to elicit recommendations for improving the quality of this ISAM.

Finally, the main research question, "*What constitutes a framework for validating methodologies designed to assess the level of (aspects of) information security within organizations?*" is answered by the combination of the answers of the subquestions. This thesis explores various methods of measuring the level of Information Security in organizations found in literature. Lacking a good definition for these various methodologies, a definition is proposed for this class of methodologies, namely ISAM. It explores Information Security standards, makes a selection of these standards and integrates them into one database, which can be used to

analyze the overall coverage of several categorizations of controls, which in turn are used in order to analyze the overall coverage of an ISAM. The suitability of this database for analyzing ISAMs is demonstrated in a case study of the State of Security assessment, which demonstrates the framework by developing a report with recommendations on how to improve the State of Security assessment.

6.2 Discussion and Limitations

This thesis follows up on the conclusion drawn from a literature review of methodologies which measure Information Security, which established that there is a need for a framework for validating such methodologies, and attempts to establish such a framework. In this thesis, multiple Information Security standards were combined into one database of controls with which Information Security Assessment Methodologies (ISAMs) can be measured and analyzed. In order to demonstrate the suitability of this framework to the main goal, an ISAM named the State of Security assessment is analyzed as a case study, and the results of this analysis are presented in this thesis.

The result of this thesis is a framework that can be used to determine the coverage of relevant Information Security standards by a ISAMs, and to elicit recommendations in order to improve the quality of the ISAM.

Due to time constraints, a subset of all major Information Security standards that were found was actually incorporated into the database. Notable omissions include PCI-DSS (the Payment Card Industry Data Security Standard) and ISA/IEC 62443 (a series of standards aimed at improving the security of ICS). A contributing factor in deciding to implement other standards first was that these standards are not universal in scope, applying mainly to organizations that process payment card information (having a focus on payment card information as a result) and organizations that use ICS.

While care has been taken to reduce the role that various forms of bias can play in the measurement of an ISAM (e.g. defining various levels to which a control can be measured and requiring evidence supporting these determinations), bias can still play a role in how an ISAM is assessed. To that end, it is recommended to have two researchers perform the measurement independently and compare their respective conclusions, if possible.

Information Security is a rapidly developing discipline, due to the cat-and-mouse game that is being played between cybercriminals and the defenders. As such, there is a lot of rapid change, which means standards change all the time as well. Indeed, since writing on this thesis began, both the CIS Controls and NIST SP 800-53 received an update, and the ISO 27001:2013 standard is up for review in 2018

as well. As a result, the set of controls that make up this database is likely subject to a lot of change. The rest of the OSSUM framework will need to be updated to reflect these changes when a standard is revised.

Finally, since the OSSUM framework relies on documented information in order to measure the coverage of an ISAM, the measurements made with the OSSUM framework may fail to measure tacit knowledge and poorly documented information. In the case of the State of Security assessment, for instance, consultants conducting the assessment are expected to have prior working knowledge of ISO 27001:2013, and the questionnaire is meant as a fall-back mechanism.

6.3 Future work

This section presents potential directions for new research following this thesis.

Future work based on this thesis could be performed in the following directions:

1. The current database only contains ISO 27001:2013, ISO 27002:2013, NIST SP 800-53r4 and the CIS Controls, with all controls being categorized according to the NIST Cybersecurity Framework. Adding new Information Security standards and categorizations may increase the breadth and depth of the framework, and the usefulness of the framework for measuring ISAMs against other standards.
2. The process of applying this framework to ISAMs is still a manual process. While it would be hard to fully automate this process due to the different meanings that various terms can have, and because computers are notoriously bad at interpretation, it may be possible to develop tooling in order to increase the researcher's efficiency. Such tools may, for instance, automatically search through text based on keywords and synonyms and present potentially relevant snippets of text to the researcher.
3. While several ISAMs are identified in this thesis, due to time constraints none of them were validated using this methodology. For some, this is unavoidable, since the papers describing the ISAM do not contain a reference to the source materials required to actually execute the ISAM, but for the remainder this may be a useful next step.
4. Due to time constraints, it was impossible to apply this framework to more ISAMs. Future work could also include applying the OSSUM framework to other ISAMs.

Bibliography

[1] Christopher J Alberts and Audrey Dorofee. *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc., 2002.

[2] Chrisanthi Avgerou. Information systems: what sort of science is it? *Omega*, 28(5):567–579, 2000.

[3] AXELOS. What is itil best practice? URL https://www.axelos.com/best-practice-solutions/itil/what-is-itil.

[4] AXELOS. *ITIL Continual Service Improvement (ITIL Lifecycle Suite)*. TSO, 2011. ISBN 9780113313082.

[5] AXELOS. *ITIL Service Design (ITIL Lifecycle Suite)*. TSO, 2011. ISBN 9780113313051.

[6] AXELOS. *ITIL Service Operation (ITIL Lifecycle Suite)*. TSO, 2011. ISBN 9780113313075.

[7] AXELOS. *ITIL Service Strategy (ITIL Lifecycle Suite)*. TSO, 2011. ISBN 9780113313044.

[8] AXELOS. *ITIL Service Transition (ITIL Lifecycle Suite)*. TSO, 2011. ISBN 9780113313068.

[9] Richard Baskerville and A Trevor Wood-Harper. Diversity in information systems action research methods. *European Journal of information systems*, 7(2): 90–107, 1998.

[10] Jakub Breier and Ladislav Hudec. Towards a security evaluation model based on security metrics. In *Proceedings of the 13th International Conference on Computer Systems and Technologies*, pages 87–94. ACM, 2012.

[11] Dave Cartwright. So, you're 'iso 27001 accredited', huh? just saying so doesn't cut it. *theregister.co.uk*, April 2017. URL https://www.theregister.co.uk/2017/04/18/protect_your_digital_enterprise_iso_27001_explainer/.

[12] Center for Internet Security. The CIS Critical Security Controls for Effective Cyber Defense - version 6.1. Technical report, SANS, 2016.

[13] Center for Internet Security. Practical Guidance for Implementing the CIS Controls. Technical Report 6.1, Center for Internet Security, 2017. URL https://www.cisecurity.org/wp-content/uploads/2017/03/Controls-Practical-Guidance-for-Web-v4.pdf.

[14] Binbin Chen, Zbigniew Kalbarczyk, David M Nicol, William H Sanders, Rui Tan, William G Temple, Nils Ole Tippenhauer, An Hoa Vu, and David KY Yau. Go with the flow: Toward workflow-oriented security assessment. In *Proceedings of the 2013 workshop on New security paradigms workshop*, pages 65–76. ACM, 2013.

[15] Paul De Hert and Vagelis Papakonstantinou. The proposed data protection regulation replacing directive 95/46/ec: A sound system for the protection of individuals. *Computer Law & Security Review*, 28(2):130–142, 2012.

[16] Energy Department for Business and Industrial Strategy. Business population estimates. Technical report, UK Government, 2016.

[17] Dimensional Research. Trends in security framework adoption: a survey of it and security professionals. 2016. URL http://www.tenable.com/press-releases/nist-cybersecurity-framework-adoption-linked-to-higher-security-confidence-according

[18] D Dresner. The iasme standard for information and cyber security. Technical Report 4.0, The IASME Consortium, 2016.

[19] Elsevier. About Scopus, 2017. URL https://www.elsevier.com/solutions/scopus.

[20] European Parliament and Council. General data protection regulation, jun 2016. Regulation (EU) 2016/679.

[21] James E Goldman and Suchit Ahuja. Integration of cobit, balanced scorecard and sse-cmm as a strategic information security management (ism) framework. In *Proceedings of the 10th Annual Information Security Symposium*, page 19. CERIAS-Purdue University, 2009.

[22] James E Goldman and Vaughn R Christie. Metrics based security assessment. *Information security and ethics: social and organizational issues*, page 261, 2005.

[23] Jonas Hallberg, Amund Hunstad, and Mikael Peterson. A framework for system security assessment. In *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC*, pages 224–231. IEEE, 2005.

[24] E Henson and D Booth. Information assurance and smes: Research findings to inform the development of the iasme model, 2010.

[25] Richard Henson, Daniel Dresner, and David Booth. Iasme: Information security management evolution for smes. 2011.

[26] ISA. Overview - the 62443 series of standards - industrial automation and control systems security. Technical report, ISA, 2015.

[27] ISACA. Glossary of terms. URL https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf.

[28] Isaca. *Cobit 3*. ISA, 2000. ISBN 1893209148, 9781893209145.

[29] Isaca. *Cobit 5*. ISA, 2012. ISBN 1604202378, 9781604202373.

[30] ISACA. Cobit 5 for information security. Technical report, ISACA, 2012.

[31] ISO. ISO/IEC 27000 family - Information security management systems. URL https://www.iso.org/isoiec-27001-information-security.html.

[32] ISO. Information technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM). Standard, International Organization for Standardization, 2008.

[33] ISO. Information security management systems - Requirements. Standard, International Organization for Standardization, 2013.

[34] ISO. Code of practice for information security controls. Standard, International Organization for Standardization, 2013.

[35] ISO. Information security management systems - Overview and vocabulary. Standard, International Organization for Standardization, 2016.

[36] ISO. The iso survey, 2017. URLhttps://www.iso.org/the-iso-survey.html.

[37] Meiko Jensen, Jörg Schwenk, Nils Gruschka, and Luigi Lo Iacono. On technical security issues in cloud computing. In *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on*, pages 109–116. IEEE, 2009.

[38] Erik Johansson and Pontus Johnson. Assessment of enterprise information security-an architecture theory diagram definition. *Proc. of CSER*, 5, 2005.

[39] Erik Johansson and Pontus Johnson. Assessment of enterprise information security - estimating the credibility of the results. In *Proceeding of the Symposium on Requirements Engineering for Information Security (SREIS) in the 13th International IEEE Requirements Engineering Conference*, volume 13, 2005.

[40] Erik Johansson and Pontus Johnson. Assessment of enterprise information security - the importance of prioritization. In *EDOC Enterprise Computing Conference, 2005 Ninth IEEE International*, pages 207–218. IEEE, 2005.

[41] Erik Johansson, Mathias Ekstedt, and Pontus Johnson. Assessment of enterprise information security the importance of information search cost. In *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on*, volume 9, pages 219a–219a. IEEE, 2006.

[42] Dejan Kosutic. *9 Steps to Cybersecurity*. EPPS Services Ltd, Zagreb, 1 edition, 2012. ISBN 9789535745204.

[43] Dejan Kosutic. Cybersecurity framework vs. iso 27001 which one to choose?, feb 2014. URL https://advisera.com/27001academy/blog/2014/02/24/which-one-to-go-with-cybersecurity-framework-or-iso-27001/.

[44] Simon Liu and Rick Kuhn. Data loss prevention. *IT professional*, 12(2), 2010.

[45] Dan Lohrman. Nist cybersecurity framework: Five reasons why it matters for your infrastructure. *govtech.com*, February 2014. URL http://www.govtech.com/blogs/lohrmann-on-cybersecurity/NIST-Cybersecurity-Framework-Five-reasons-why-it-matters-for-your-infrastructure.html.

[46] Zaigham Mahmood. Data location and security issues in cloud computing. In *Emerging Intelligent Data and Web Technologies (EIDWT), 2011 International Conference on*, pages 49–54. IEEE, 2011.

[47] Derek Manky. Cybercrime as a service: a very modern business. *Computer Fraud & Security*, 2013(6):9–13, 2013.

[48] Oleksiy Mazhelis and Hannakaisa Isomäki. Security assessment and planning in small organizations. In *INC*, pages 149–159, 2008.

[49] Merriam Webster. Standard, 2017. URL https://www.merriam-webster.com/dictionary/standard.

[50] Daniel L Moody, Maria Eugenia Iacob, and Chintan Amrit. In search of paradigms: identifying the theoretical foundations of the is field. In *Proceedings of ECIS 2010*. University of Twente, 2010.

[51] NIST. Nist sp 800-53. *Security and Privacy Controls for Federal Information Systems and Organizations*, apr 2013.

[52] NIST. Framework for improving critical infrastructure cybersecurity. Technical report, NIST, 2014.

[53] NIST. Nist general information, mar 2017. URL https://www.nist.gov/director/pao/nist-general-information.

[54] NIST. Nist computer security publications - nist special publications (sps), jun 2017. URL http://csrc.nist.gov/publications/PubsSPs.html.

[55] SP NIST. 800-37, revision 1. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, 16, 2010.

[56] Chitu Okoli and Kira Schabram. A guide to conducting a systematic literature review of information systems research. *Sprouts Work. Pap. Inf. Syst*, 10(26), 2010.

[57] Organisation for Economic Co-operation and Development. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. OECD Publishing, 2002.

[58] Donn B Parker. Toward a new framework for information security? *Computer Security Handbook, Sixth Edition*, pages 3–1, 2002.

[59] Ken Peffers, Tuure Tuunanen, Marcus A Rothenberger, and Samir Chatterjee. A design science research methodology for information systems research. *Journal of management information systems*, 24(3):45–77, 2007.

[60] Chad Perrin. The cia triad. *Dostopno na: http://www. techrepublic. com/blog/security/the-cia-triad/488*, 2008.

[61] Sasko Ristov, Marjan Gusev, and Magdalena Kostoska. A new methodology for security evaluation in cloud computing. In *MIPRO, 2012 Proceedings of the 35th International Convention*, pages 1484–1489. IEEE, 2012.

[62] Manuel Rudolph and Reinhard Schwarz. A critical survey of security indicator approaches. In *2012 Seventh International Conference on Availability, Reliability and Security (ARES)*, pages 291–300. IEEE, 2012.

[63] SANS Institute. Sans institute: About. URL https://www.sans.org/about/.

[64] Maung K Sein, Ola Henfridsson, Sandeep Purao, Matti Rossi, and Rikard Lindgren. Action design research. *MIS quarterly*, pages 37–56, 2011.

[65] Mikko Siponen and Robert Willison. Information security management standards: Problems and solutions. *Information & Management*, 46(5):267–270, 2009.

[66] Heather Skinner. Action research. In *Formative Research in Social Marketing*, pages 11–31. Springer, 2017.

[67] Software Engineering Institute. A systems engineering capability maturity model. Technical Report 1.1, Carnegie Mellon University, 1995.

[68] Ernest T Stringer. *Action research*. Sage Publications, 2013.

[69] Richard G Taylor. Potential problems with information security risk assessments. *Information Security Journal: A Global Perspective*, 24(4-6):177–184, 2015.

[70] Daniel Tse. Security in modern business: security assessment model for information security practices. *PACIS 2004 Proceedings*, page 119, 2004.

[71] Rossouw von Solms, H Van Der Haar, Sebastiaan H von Solms, and William J Caelli. A framework for information security evaluation. *Information & Management*, 26(3):143–153, 1994.

[72] Lawrence M. Walsh. March 2002 - features - security standards - standard practice - iso 17799 aims to provide best practices for security, but leaves many yearning for more. *Information Security magazine*, Mar 2002. URL https://web.archive.org/web/20020605134918/http://www.infosecuritymag.com/2002/mar/iso17799.shtml.

[73] Andy Ju An Wang. Information security models and metrics. In *Proceedings of the 43rd annual Southeast regional conference-Volume 2*, pages 178–184. ACM, 2005.

[74] Wikimedia Commons. The cia triad, 2009. URL https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png.

[75] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. Iot security: ongoing challenges and research opportunities. In *Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on*, pages 230–234. IEEE, 2014.