Information security for Industry 4.0

A framework to aid manufacturing SMEs with implementing information security measures for Industry 4.0 technologies

Lorenzo Desmedt

Student number: 2021060

Supervisors: Joris Hulstijn (Tilburg University)

Frederik Boot (Baker Tilly)

A thesis presented for the degree of

Master of Science in Information Management

Tilburg School of Economics and Management

Tilburg University

The Netherlands

June 09, 2022

Management Summary

Industry 4.0 technologies, such as Internet of Things, cloud solutions and Big Data, are being implemented more and more often. The implementation of Industry 4.0 technologies in manufacturing SMEs willing to transform comes with a change in the role of data in a firm. These technologies create, transfer and store a large amount of data in new ways compared to not having implemented the technology. This opens the firm up to exposure of new types of risks, including information security risks.

Due to there being no specific framework available for the implementation of Industry 4.0 technologies in SMEs regarding information security. An opportunity lies here to fill the gap that exists between these areas.

In this research project, we aim to help manufacturing SMEs with the implementation of a baseline of information security measures during and after the implementation of Industry 4.0 technologies using a framework. This is done by understanding how the technologies influence information security, finding out which measures are needed to solve this, and combining these factors to create the framework. To give a clear overview of the value of each measure, the measures are divided into the elements of the CIA Triad, namely; Confidentiality, Integrity and Availability.

To gather data on this subject, five interviews and 81 papers and other sources were used. The interviews gave a view in to the real-world where businesses deal with information security in many different ways and on many different levels. The sources were used for gathering information about the technologies and information security.

After the primary and secondary data were processed, the framework was developed. The framework is based on the best practices of seven existing information security frameworks, with CIS Security Controls being the biggest source, as well as the literature and interviews.

The initial framework was validated by three experts in the field of information security to assess the completeness, usefulness and usability of the framework. After this validation, the framework was adjusted and finalized.

This research contributes both practically and academically. The practical contribution is an information security framework which gives manufacturing SMEs the possibility to implement a baseline of information security measures during and after the implementation of Internet of Things, cloud solutions and/or Big Data. This research contributes academically by being the first research to focus on a baseline of information security measures in the context of Industry 4.0.

Preface

In front of you lies my master thesis: “Information security for Industry 4.0: A framework to aid manufacturing SMEs with implementing information security measures for Industry 4.0 technologies”.

This thesis was written during the second and last semester of my master study in Information Management at the University of Tilburg. I will admit that, although the world has been gradually opening up after a, hopefully, once in a generation pandemic, this research has been the most difficult academic assignment I have yet experienced. It gave me a lot of joy learning about numerous new subjects, whilst also for the first time gaining the experience of an internship.

I would like to thank all of the colleagues and fellow interns at Baker Tilly for their guidance, time and motivation. I would especially like to thank Frederik Boot, my supervisor at Baker Tilly, for all his advice and knowledge, but also stories and kindness. Frederik was always available for questions and has also taught me a lot about the business that is Baker Tilly.

I would also like to thank Joris Hulstijn, my supervisor, for his guidance and feedback during this period. The advice Joris gave during our meetings pushed me in the right direction to create the thesis as it is now.

Ultimately, I can say that the end product this thesis has become is vastly different from what I had imagined at the start of this adventure. This, however, does not mean I am unsatisfied with the end product. The opposite is entirely true, I could not have imagined a more fitting artifact to reflect my knowledge and experiences.

I hope this thesis will be enjoyable and informative, even more so than the project was for me.

Lorenzo Desmedt

Middelburg, June 09, 2022

Table of Contents

1. Introduction

This chapter introduces the problems businesses face when implementing information security measures during and after the implementation of Industry 4.0 technologies. After the introduction of the problem, the research questions will be explained. Finally, the research method of this thesis is explained together with a diagram of the conceptual model of this thesis.

1.1 Problem Indication

When in the late 18th century, the introduction of water and steam powered machines caused an increase of production efficiency and scale, the world got to know it's first major industrial revolution. More than two centuries later, a so-called 'fourth industrial revolution' takes place with the rapid change to interconnectivity and smart automation in a cyber-physical transformation of manufacturing (Erboz, 2017; Lee et al., 2015). This fourth industrial revolution is a strategic initiative introduced by the German government (Rojko, 2017). This Industry 4.0, or I4.0 for short, as it was coined by German researcher Wolfgang Wahlster (*Professor Wolfgang Wahlster*, n.d.), contains nine pillars; Big Data, autonomous robots, simulation, additive manufacturing, Internet of Things, cloud computing, augmented reality, horizontal and vertical integration and cybersecurity (Erboz, 2017). This thesis will focus on three of the major component technologies of Industry 4.0, which were expected to have the most profound impact on an organization (Deloitte Global analytics, 2020). These are Internet of Things, cloud infrastructure and Big Data.

Defined as enterprises with less than 250 employees, and less than €50 million turnover or less than €43 million balance sheet total, small and medium-sized enterprises (SMEs) represent 99% of all businesses in the EU (European Commission, n.d.). Although this group has an overwhelming majority, individually they are at a disadvantage compared to the other, larger enterprises. This is due to a lack of "resources and expertise in terms of management of new technologies" (Blili and Raymond, 1993). "However", Blili and Raymond continue, "this does not necessarily mean that IT is the exclusive property of big business." This disadvantage does result in "the adoption rate of the technology in SMEs [being] slower than in larger companies" (Awwad et al., 2020). An exception for this is, for example, the ease with which certain SMEs can implement cloud solutions, such as storage, computing and services. Additionally, Masood and Sonntag (2020) found, in their sample of SMEs in the manufacturing sector, that "Whilst many SMEs show a desire to implement Industry 4.0 technologies […], financial and knowledge constraints are found to be key challenges." On the other hand, there are a number of advantages SMEs have over larger enterprises, namely the flexibility and lack of bureaucracy in decision making. My expectation is that SMEs are more capable in the implementation of Industry 4.0 technologies than they think and that IT is there for every type of

business, but a helping hand and an informative guide about the technologies are needed to get those struggling on their way. This helping hand will need to reduce some cost otherwise spent by SMEs on research and give knowledge to overcome the key challenges Masood and Sonntag (2020) found.

These facts do not only make SMEs interesting to study, they also present an opportunity for the creation of a reference framework designed to aid SMEs by reducing the knowledge constraint. This framework will help the SMEs with providing theory about the exploration and implementation of information security measures for certain Industry 4.0 technologies, namely: Internet of Things, cloud infrastructure and Big Data. Specifically, this thesis will look at the manufacturing subset of the SMEs. This is due to the definition of Industry 4.0, as this refers to the cyber-physical transformation of manufacturing (Erboz, 2017; Lee et al., 2015).

The implementation of Industry 4.0 technologies in manufacturing SMEs willing to transform comes with a change in the role of data in a firm. This opens the firm up to exposure of new types of risks, including information security risks. Data will, in most cases, become more important for daily operations and decision making. In order to facilitate this, a firm may need to redesign their data infrastructure, including storage, permissions and encryption. Information security frameworks containing standards for these issues exist, like the ISO/IEC 27001 and NIST Cyber Security Framework (ISO/IEC, 2013a, 2013b; NIST, 2018). Such standards contain a large number of general measures which a business can adapt to their situation and implement where applicable.

Data infrastructure redesign needs to be done according to information security frameworks in order to prevent security risks from occurring, resulting in loss or exposure of data. A disadvantage of the use of general information security frameworks for Industry 4.0 is the lack of coverage of the new technologies (IoT, Cloud and Big Data), which require specific elements to be addressed (ISO/IEC, 2013a, 2013b; NIST, 2018). This lack of coverage results in SMEs having to use and dissect a number of information security frameworks in order to find the elements which they deem important, without having expert knowledge about information security. This can result in higher costs and/or incomplete information security.

To set the scope of this thesis, the framework which will help manufacturing SMEs with information security during and after the implementation of Industry 4.0 technologies will be based on the CIA Triad: confidentiality, integrity and availability. “The CIA Triad […] refers originally to the fundamental elements of security controls in information systems” (Samonas & Coss, 2014). Its parts: confidentiality, integrity and availability each affect a different part of information security. The first part, confidentiality, concerns itself with keeping sensitive information protected. This can be seen as information being on a ‘need to know’ basis, where only authorized people are able to access and

see the information, like role-based access control. For this reason, confidentiality also concerns itself with the prevention of phishing and hacking attempts, to name only a few possible ways in which data can be stolen. The second part, integrity, concerns itself with preventing unauthorized people from manipulating stored information and making authorized people behave responsibly according to policies and procedures, which could otherwise make the information incorrect and not sound. When transferring data, measures must also be in place to prevent alteration of the data. The third and final part, availability, concerns itself with keeping information available and accessible to authorized parties. For this reason, availability concerns itself with the maintenance of hardware, technical infrastructure and systems which contain, transfer or present information. This is in order to keep these systems up and running. Availability also concerns itself with prevention of attacks which disable or hinder correct operation of the aforementioned maintenance areas. Finally, availability deals with redundancy in infrastructure and back-up and recovery, to prevent moments of unavailability of the systems and data.

There is recent knowledge about the readiness of SMEs for Industry 4.0 technologies. Safar et al. (2018) introduced a business model for the early guidance of SMEs "which should represent [a] backbone for planning new businesses in [the] Industry 4.0 environment or rebuilding the already existing businesses." This early guidance model should give businesses a solid foundation, but it does not give any real method for implementing this model. This reduces the practicality of the model. Safar et al (2018) suggest that the implementation of cloud storage as the first step for implementing an Industry 4.0 platform as this is a faster and cheaper option of providing machines the infrastructure to talk to each other, also called interoperability.

Additionally, there is some knowledge about the security vulnerabilities and challenges which can follow from the implementation of Industry 4.0 technologies, as shown by Andrea et al. (2015). Andrea et al. (2015) conclude that the rapid progression of IoT came with many security and privacy threats, hindering development. Measures for successfully securing an IoT system were also highlighted.

A literature study by Orzes et al. (2018) found that in the literature, a lack of standards about the implementation of Industry 4.0 in SMEs and data security concerns were the most published subjects. This is likely due to the changing role of data, making it unclear which standards to follow. Additionally, the current information security standards are not specific enough to present a solution for every situation. This implies that more research about these subjects is needed in the literature.

Due to there being no specific framework available for the implementation of Industry 4.0 technologies in SMEs regarding information security. An opportunity lies here to fill the gap that exists between these areas.

1.2 Problem Statement

As mentioned in the problem introduction, SMEs have financial constraints and a lack of knowledge when it comes to the information security risks that come with the implementation of new technologies. These constraints require the SMEs to find external help to investigate whether the information security is sufficient in the organization or not. Not seeking help when no internal IT support is available, can result in security breaches due to wrongly implemented measures or forgotten measures. This possible need for help will then also continue into the implementation part, as SMEs often lack expertise for the management of these new technologies.

With the constraints that SMEs face and the growing importance of business information, a solution is needed to help SMEs discover which steps and requirements are needed during and after the implementation of new technologies whilst keeping their business information secure.

Therefore, this thesis aims to create a basic framework which helps SMEs keep their business information secure during and after the implementation of Industry 4.0 technologies by providing a number of information security measures. The framework will contain the measures needed to be implemented to create a solid baseline information security foundation, without needing to be completely adapted for the specific business. It will need to be usable by anybody with some IT knowledge but without the need for external help from consultants.

The scope of this research focuses on information security during and after Industry 4.0 technology implementation in SMEs. The duration of the research has been limited to 5 months. Participants of the research are limited to employees and clients of Baker Tilly.

The scope of the research has several limitations, such as:

- Limited number of technologies researched.
- Higher focus on prevention than on resilience.
- Focus on individual enterprises, not entire networks.
- Focus only on manufacturing SMEs, not all types of SMEs.
- Insufficient time to fully test the framework, only expert feedback for validation.

This framework will be created using a risk-based approach. This is done to provide a clear overview of the risks which need to be mitigated. In practice, this will be done by using the CIA Triad and mapping measures needed to mitigate risks on the different aspects of the CIA Triad.

1.3 Research Question

“How can information be kept secure with a risk-based approach when implementing Industry 4.0 technologies in the SME manufacturing industry?”

Sub-questions:

1. What are the components and what is the value of the chosen Industry 4.0 technologies?
2. How do these components influence data security in a SME?
3. Which measures lay the basis for solid information security?

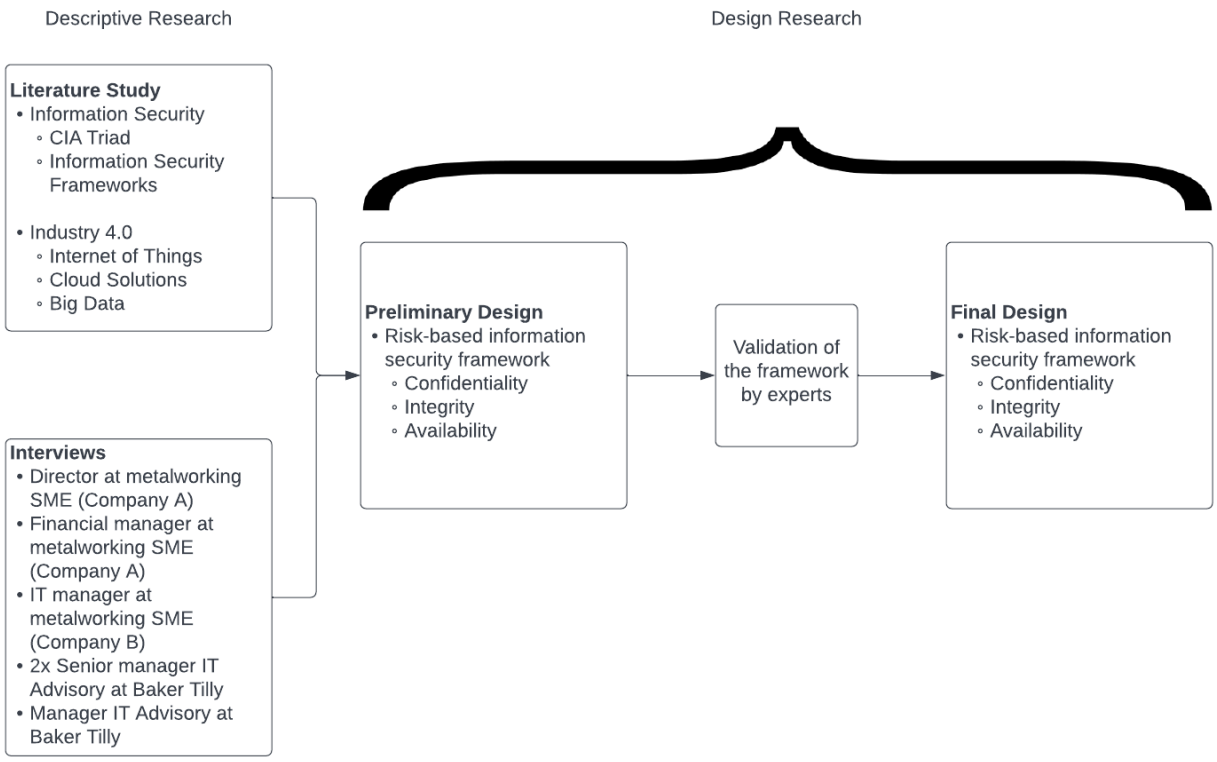
1.4 Research Method

This research consists of two parts: a descriptive research part and a design research part. In the descriptive research part specific components of Industry 4.0, information security and the CIA Triad will be discussed. Specifically, Internet of Things, cloud infrastructure and Big Data will be discussed as a part of Industry 4.0. This will be achieved using literature reviews, interviews and case studies. In the design research part, a framework will be developed which can be used by SMEs before and during the implementation of Industry 4.0 technologies to help keep their information security up. This framework will be validated by experts and possibly revised according to their feedback.

In order to make the quick refamiliarization with the conceptual model easier, a diagram has been added below.

Figure 1

Diagram of the conceptual model of this thesis.



Note. The experts who will provide validation are the same expert manager and expert senior managers who were interviewed.

2. Literature Review

This chapter examines the existing literature in order to comprehend the main topic of this thesis. This is done in two parts, information security and Industry 4.0. These parts will provide familiarity with the topic in order to help develop a reliable and valid framework. The selection of sources is described in chapter 3.3.

2.1 Information Security

Information security concerns itself with the protection of sensitive information from unauthorized activities. These activities include, but are not limited to: inspection, modification, recording, disruption and destruction. Any breach of information security can result in the inability of an organization to function, be it due to loss of data or otherwise.

2.1.1 CIA Triad

Three principles of information security are the so-called CIA Triad (Bell et al., 1973; Clark & Wilson, 1987; ISO/IEC, 2013a). The CIA Triad consists of confidentiality, integrity and availability. When applicable, each of these three principles must be implemented in an organization or program to ensure proper information security. This includes the adaptation of these principles in the event of the introduction of a new element or technology in an organization.

Over the years, the academic view towards information security has changed due to the evolution in information security. This change was represented by the introduction of eight different terms and concepts complementary to the CIA Triad in academic literature (Samonas & Coss, 2014). These terms are: authenticity, non-repudiation, correctness of specification, responsibility, integrity of people, trust, ethicality and identity management. Over a space of some 40 years, these terms and concepts were introduced. Samonas & Coss (2014) argue that “50 years after its conception, the CIA Triad will still be uniquely relevant for security practitioners and will continue to serve as a point of reference in security management.” This is due to the possibility to incorporate any of the eight additions of the CIA Triad within a broad interpretation of the original three elements: confidentiality, integrity and availability. Samonas & Coss (2014) illustrate this by adopting an etymological interpretation of the original three elements of the CIA Triad, and review these in relation to the eight additions that have been discussed in academic literature over the years. In the paper, Samonas & Coss (2014, p. 30) present these findings as seen in table 1.

Table 1

Classification of additional tenets to the original CIA triad.

Additional Tenets	Relation to CIA Triad
Authenticity	Integrity
Non-repudiation	Integrity
Correctness in specification	Integrity and Availability
Responsibility	Integrity
Integrity of people	Integrity
Trust	Confidentiality and Integrity
Ethicality	Integrity
Identity management	Confidentiality, Integrity and Availability

Note. Reprinted from Samonas and Coss (2014).

The classification by Samonas & Coss (2014) will give the possibility to focus on confidentiality, integrity and availability, by grouping the other elements within the original CIA Triad. This will mean that when one of the eight additional tenets is mentioned or discussed, it will be done so via the classification as seen in table 1.

The following chapters will explain the definitions and uses of each of the three parts of the CIA Triad. Additionally, best practices and their influence will be discussed.

2.1.1.1 Confidentiality

The first part of the CIA Triad, confidentiality, concerns itself with the protection of sensitive information. Meaning that in every scenario, information is secure and only accessible to individuals who are authorized to do so.

Measures to ensure proper confidentiality can be split into two groups. The first group contains measures to ensure that the person that accesses the data, is the person they claim to be. The second group contains measures to ensure that if the data is stolen and falls into the wrong hands, the attackers are unable to use the data.

Some of many measures possible in the first group are periodic changing of the password, not using a password on multiple sites, two factor authentication and biometric verification. The first two measures are specifically aimed at Conversely, Herley (2009) argues that periodic changing will only work when “the attacker waits weeks before exploiting the password”, and therefore is of marginal benefit. Additionally, Florêncio and Herley (2007) state that on average, a password is being used at 3.9 different sites by a single user. Aloul et al. (2009) mention that “by definition, authentication is the use of one or more mechanisms to prove that you are who you claim to be. Once the identity of

the human or machine is validated, access is granted." Aloul et al. (2009) continue to explain that there are three "universally recognized authentication factors", namely: what you know (e.g., passwords), what you have (e.g., ATM card), and what you are (e.g., biometrics). Biometrics can be implemented in a hands-free operation with the use of voice recognition or eye scan.

The two-factor authentication system uses two of the aforementioned mechanisms to strengthen the security of the system. Most people will only come by a two-factor authentication system using something they know and have, such as an ATM card and PIN number for transactions. Due to the cost and complexity of the implementation and maintenance of a biometric verification system, these are rarely used for public use, such as an ATM (Aloul et al., 2009). This is also why biometric verification can be seen as a separate authentication system, given the rarity of use. This rarity of use does not mean that biometric verification is impossible, as was proven by Lin and Fan (2004). The advantage of the use of biometric verification is the added level of security, but it comes at a higher cost than the other two authentication factors. Additionally, in the case the biometrics of an individual are stolen or copied, it is nearly impossible to change the security system to distinguish between the real and fake biometrics. This means that companies and their employees must be very careful not to let the biometrics fall into the wrong hands, as the biometrics cannot be changed, unlike a password.

For the second group, most measures will be represented by data encryption. Data encryption can be split into three parts: in transit, in use and at rest. Each of these types will have a unique encryption method, like symmetric encryption, asymmetric encryption or AES-encrypted portable media. Whichever method is chosen, for example, data encryption in transit will always come to the same conclusion: ensure that the sender and receiver(s) of information are the only ones that can access and read the data. According to Kerckhoffs's principle (1883), an encrypted system should be secure, even if everything about the system, except the key, is public knowledge. Therefore, ensuring that the key, which is used to decrypt the data, is safe and secure, is very important for data encryption. This principle is not correct when using symmetric encryption, as this uses a single key, which needs to be kept secret. Asymmetric encryption uses a key pair, which uses a non-secret public key (Daniel, 2021).

2.1.1.2 Integrity

The second part of the CIA Triad, integrity, concerns itself with maintaining the consistency, trustworthiness and accuracy of data over its entire lifecycle (Clark & Wilson, 1987; Grefen & Apers, 1993). This includes the prevention of data corruption and unexpected and unauthorized data modifications.

Grefen and Apers (1993) present four classes from which information integrity violations can occur: security control, concurrency control, reliability control and integrity control. Security control deals with authorization of users. “Concurrency control deals with prevention of inconsistencies caused by concurrent access of multiple users” (Grefen & Apers, 1993). Reliability control deals with hardware or software errors. “Integrity control deals with the prevention of semantic errors made by users due to their carelessness or lack of knowledge” (Grefen & Apers, 1993). Sivathanu et al. (2005) address that “[with] most systems that do not have integrity assurance mechanisms, unexpected modifications to data either go undetected, or are not properly handled […], resulting in software crash or further damage to data.”

In order to prevent loss of data integrity due to any type of violation, multiple measures can be put in place. Firstly, to prevent malicious activities such as unauthorized data modifications, all users of a system must have proper rights and permissions allocated to their account. This will not allow users to edit data which they are not allocated to change. Secondly, to prevent integrity violations due to hardware or software malfunctions, inadvertent user errors or non-human threats like an electromagnetic pulse or server crash, multiple measures can be taken, like mirroring and RAID parity (Sivathanu et al., 2005).

Mirroring is the replication of data and comparing the two versions to investigate whether any integrity violations are present. This solution is easy to implement according to Sivathanu et al. (2005), but this method is inefficient both in terms of storage space and time. Mirroring can detect integrity problems due to hardware errors, but cannot revert the data to the correct original as the correct version of the data is unknown to the program. This can in turn be prevented by making two copies and using a majority vote to find the correct data. This will make mirroring even more inefficient.

RAID parity is a way to prevent loss of data due to hardware failure by efficiently copying data and distributing over multiple drives (Sivathanu et al., 2005). This will use more space than the data by itself would, but prevents total data loss in the case that a part of the storage drives are lost. Although this can be seen as system integrity, it does prevent the information integrity from being violated.

Finally, non-repudiation, a kind of digital signature, provides proof of origin of data. The signature assures the sender that their message is received, whilst providing the recipient with the sender’s identity. This prevents either party from denying that the message was sent, received and processed (Awati, 2021).

2.1.1.3 Availability

The third and final part of the CIA Triad, availability, deals with the guarantee that there is consistent access to all information according to specifications. This includes the maintenance of software, hardware and technical infrastructure and systems responsible for the presentation of the information.

According to Qadir and Quadri (2016), availability is the least discussed and researched attribute of information security. But, Qadir and Quadri (2016) continue; "this does not certainly mean that it is the least important attribute of Information Security. In fact, it plays an important role in determining the other attributes of Information Security (confidentiality and integrity), because these two attributes are directly dependent upon the Availability." Qadir and Quadri (2016) continue to argue that without availability of information, confidentiality and integrity of the information is not needed.

Multiple measures are possible to implement to keep the availability of information reliable. Firstly, maintaining and repairing hardware, and assuring that the operating system is operational, up to date and without conflicts. Secondly, ensuring that the bandwidth is sufficient to prevent bottlenecks, due to which users otherwise have to wait longer for data to be presented. Thirdly, fast disaster recovery is also essential. This recovery has the task of ensuring that a sudden partial or complete loss of data availability will be repaired as soon as possible. Finally, being able to fall back on a paper procedure can help to prevent complete loss of information availability. Plans formulated in the Business Continuity Management (BCM) procedure can be used for inspiration for these measures. This can also be an inspiration point for the creation of the BCM.

Separately, Ranganathan et al. (2002) address a measure which helps improve availability in unreliable systems, namely replication. Similarly to mirroring to improve integrity, replication requires multiple copies of data on independent nodes. This will increase the chance of at least one of the nodes, and therefore data, being accessible at any time.

2.1.2 Costs of Breaches

The cost of a breach of information security will vary per company based on the size of the breach, the dependency on data and ability to respond. Layton and Watters (2014, p. 322) and Cavusoglu et al. (2004) separate the cost of a data breach into tangible and intangible costs.

Cavusoglu et al. (2004) also present another way to broadly classify costs of security breaches. This classification into transitory (short-term) and permanent (long-term) separates the costs based on whether are "incurred only during the period in which the breach occurs […] [or] are incurred after the immediate effects of the breach are dealt with" (Cavusoglu et al., 2004, p. 67).

Based on Layton and Watters (2014, p. 322) and Cavusoglu et al. (2004, pp. 66-68), table 2 presents different costs separated based on their tangibility and time of occurrence.

Table 2

Costs of information security breaches.

	Transitory (short-term)	Permanent (long-term)
Tangible	• Investigation costs • Data restoration • Legal costs • Media costs	• Additional information security staff • Increased interest rates • Increased insurance rates
Intangible	• Criminal charges • Opportunity costs • Loss of staff & productivity • Increased risk of future attacks	• Loss of reputation • Loss of customers • Inability to attract new customers • Loss of trust in stakeholders

Note. Adapted from Layton and Watters (2014).

Relevancy of these costs will differ whether the confidentiality, integrity and/or availability of the data is breached. Cavusoglu et al. (2004) conclude that "intangible costs of security breaches can be much larger than the tangible costs." Therefore, firms ignoring intangible costs are grossly underestimating the total costs of a security breach. This can result in under-investments in IT security, in turn increasing the odds of an information security breach.

Conversely, Layton and Watters (2014) argue that intangible costs are "overstated and […] not as significant as it is thought to be." This is based on short term stock prices of companies affected by data breaches. Layton and Watters (2014) continue to say that "share price and company reputation are not perfectly correlated" and that "harm to reputation may occur over the long term" which limits the argument they present.

The degree of uncertainty in the estimation of the costs of a security breach is dependent on the classification of the costs. Cavusoglu et al. (2004) present table 3 for the degree of uncertainty.

Table 3

Degree of uncertainty in estimation of costs.

	Transitory	Permanent
Tangible	*Low*	*High*
Intangible	*High*	*Very High*

Note. Reprinted from Cavusoglu et al. (2004).

2.1.3 Information Security Breach Examples

In the past decades, the amount of malware encountered in companies has grown, often with the goal of getting a ransom from the company, also called ransomware. Sometimes, the makers of this malware have other goals in mind, as can be seen in the Stuxnet example.

Kushner (2013) wrote a summary of the events that follow the story of Stuxnet, which will be used as the main source for this example. Stuxnet is a 500-kilobyte computer worm which, when discovered in 2010, had infected at least 14 Iranian industrial sites. One of these sites was a uranium-enrichment plant. After Stuxnet entered a system via USB stick, it infected every machine using Microsoft Windows. When Stuxnet found itself in the right machines, it updated itself and went on the compromise vulnerabilities that were not yet discovered by security experts. This allowed Stuxnet to spy on the operations and learn to take control of, in this instance, centrifuges, allowing them to spin at speeds too high for the centrifuge to handle, resulting in failure of the machines. This all was being done whilst presenting feedback which would indicate normal operation, instead of imminent failure. Officially, no actual damages were caused by the malware, but, according to the Institute for Science and International Security and International Atomic Energy Agency, the Iranian nuclear program was delayed by one year. Chen and Abu-Nimeh (2011, p. 93) present three lessons to be learned from Stuxnet: “malware can affect critical physical infrastructures”, “isolation from the internet isn’t an effective defense” and “an extremely motivated attacker might have an unexpected combination of inside knowledge, advanced skills, and vast resources.”

An example of malware with the intention of receiving a ransom from a company is the cyberattack on the VDL group in October 2021. This attack ended up preventing production of cars for a number of days, costing many millions of euros. Thanks to back-ups created less than a day before the cyberattack hit the systems, at most one day’s worth of data was lost. The VDL group did not present any more information regarding the cyberattack and IT-systems (Monterie, 2021). This attack reinforces the importance of data back-ups and information security in general.

In 2018, one of the largest data breaches in the world occurred. The Aadhaar data breach was a breach data of hundreds of millions to a billion people in India. This Indian government run database containing personal information and biometric data had multiple leaks in the security, providing the possibility of finding the data through a simple Google search. Additionally, the Android mobile phone application, downloadable through the Google Play Store, contained a number of security bugs allowing hackers to enter the database (All Answers Ltd, 2021). This data breach was caused by many mistakes and faults in the information security, and it proves that sufficient information security is absolutely needed, especially if you store personal information.

The importance of encryption of personal data can be seen by investigating the Adobe data breach in 2013. In this breach credit card numbers, social security numbers and more of over 150 million customers of Adobe were stolen (Hern, 2017; Steve, 2020). If the confidentiality of the information was of a high standard, the hackers would not be able to use the data, as it would have been encrypted. The issue that Adobe's IT security staff made, is that all passwords were encrypted using the same encryption function. This would give hackers who cracked the encryption function easy access to every password. Additionally, this also means that a password, such as '123456', would have been encrypted as 'Eh7J2ld3FG' for every person with that password. This in itself would not necessarily give the hackers any passwords, but would give a hacker every similar password by hacking just a single password. The final and possibly worst mistake is not encrypting the password hints, which users can enter to give themselves a hint towards their password in case they forgot it. The problem with the password hints at Adobe was that a user could enter their password as a password hint, providing themselves with the password without having to think about what the hint meant. This also meant that the hackers could see the password of users who entered their password as their password hint. Steve (2020) concludes the lessons to be learned from the Adobe breach as follows: remind customers to not use a password twice, force customers to enter a lengthy and complex password, and IT security professionals should never be lazy and make the information security worse by implementing inadequate security methods.

The examples presented are of quite large companies, but the lessons learned can be applied to any size company. SMEs should therefore also try to prevent hackers or malware in every way possible, as, according to SIDN business developer Alex van Wijhe, putting ransomware on SME systems and requesting tens to hundreds of thousands of euros is a lucrative business case for cybercriminals (De Ondernemer, 2020).

2.1.4 Information Security Frameworks

In this chapter, a number of information security frameworks will be discussed and summarized. In a chapter 5.2, these summaries will be used to gain a list of best practices and minimal needs in information security frameworks. This list will function as a basis for the framework which will be created in this thesis.

The following information security frameworks will be discussed:

- ISO/IEC 27001 & ISO/IEC 27002
- NIST Cyber Security Framework
- NIST SP 800-53
- NIST SP 800-171

- COBIT
- CIS Security Controls
- Payment Card Industry Data Security Standard (PCI DSS)

ISO/IEC 27001 and ISO/IEC 27002 are part of the ISO/IEC 27000 series. The ISO/IEC 27000 series currently contains 60 standards related to information technology and security techniques. These standards are assigned a type: preventive, detective or corrective (Bowell, 2021). The ISO/IEC 27001 "provides a framework to help organizations, of any size or any industry, to protect their information in a systematic and cost-effective way, through the adoption of an Information Security Management System (ISMS)" (27001 Academy, n.d.). ISO/IEC 27002 contains and provides best practices for information security controls to be used when implementing or maintaining the ISMS. The ISO/IEC 27002 is not required when using ISO/IEC 27001, but it is an expansion which can make the use of ISE/IEC 27001 easier and faster.

ISO/IEC 27001 and the ISMS which users adopt, have the goal of protecting three aspects of information: confidentiality, integrity and availability. Before businesses implement the ISO/IEC 27001, a business risk analysis has to be done. This is to identify whether any business risks are present, which would need (improved) information security. Afterwards, the protection is done by firstly finding out what potential problems with the information could arise, after which preventive measures are defined. This can be described as risk assessment followed by risk mitigation and management.

The ISO/IEC 27000 series uses a plan-do-check-act (PDCA) cycle (ERM Protect, 2019; Roncevich, 2018). This cycle, which knows its origin in the 1939 book by Shewhart (Moen & Norman, 2006; Shewhart, 1939), invites constant improvement due to the iterative nature of the cycle . This means that an enterprise continuously reassesses the current situation of their business risks and information security and acts upon this.

ISO/IEC 27001 and ISO/IEC 27002 contain 14 domains each addressing a different part of information security. These can be found summarized in table A1 in the appendix.

The National Institute of Standards and Technology, or NIST for short, is an U.S. Government funded entity which has produced a number of cybersecurity frameworks. The three most used will be discussed. These three frameworks share a lot of elements, but also have large differences in the structure and control mechanisms depending on their use case.

The NIST Cyber Security Framework can be identified by the 'identify, protect, detect, respond and recover' steps, often depicted in a circle. The framework has the goal of integrating industry standards

and best practices, provide common language and a common understanding, give guidance on risk reduction, and give advice on responding, recovering and learning from cybersecurity attacks.

The NIST Cyber Security Framework covers five critical core areas of security (NIST, 2018):

- **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities;
- **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical services;
- **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event;
- **Respond:** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident;
- **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

The role of these steps is highlighting desired outcomes and managing the risks in a way that can cooperate with the already existing processes.

The NIST Cyber Security Framework also works with implementation tiers for managing risk. The tiers are: partial (tier 1), risk informed (tier 2), repeatable (tier 3) and adaptive (tier 4). The tiers provide context on the view of the organization on cybersecurity risk and the processes already in place to manage that risk (NIST, 2018). The categories addressed by the framework can be found in the appendix in table A2. For a more detailed view, the NIST Cyber Security Framework is publicly available. Each of the categories is split into a number of subcategories, which "divide a category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each category" (NIST, 2018, p. 7).

Lastly, the NIST Cyber Security Framework results in the use of profiles which "enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities" (NIST, 2018, p. 11). The profiles can be used to describe the current state or a desired state of cybersecurity activities. The comparison of these profiles can then be used to reveal gaps which need to be addressed.

Another NIST framework, the NIST SP 800-53 framework, is specially designed to improve information security in U.S. Federal Government agencies. The NIST SP 800-53 is organized into 18 security control families derived from the NIST Cyber Security Framework. At more than ten times

the size of the NIST Cyber Security Framework these families are more broadly addressed and explained, containing more details and requirements. These can be found explained in table A3 in the appendix.

The difference with the NIST SP 800-171 framework, is that the NIST SP 800-171 relates to non-federal entities. In addition to that there are also a number of missing and different security control families between the NIST SP 800-53 and NIST SP 800-171 frameworks.

For this thesis, only the regular NIST Cyber Security Framework will be used. This is because the additional explanations and details contained within the NIST SP 800-53 and NIST SP 800-171 frameworks will not be needed.

COBIT 2019 is the successor of COBIT 5. "COBIT 5 is a governance and management framework for information and related technology that starts from stakeholder needs with regard to information and technology" (Bernard, 2012). The update from COBIT 5 to COBIT 2019 was done because of new technology and business trends having to be incorporated into the COBIT framework. There was also a need for the "integration of new insights from practitioners, science and academia in the domain of I&T governance creation" (ISACA, 2019).

The use of COBIT 2019 is for every type of enterprise, including non-profit and the public sector. The COBIT 2019 framework lets enterprises create and extract optimal value from their information and technology. The framework is based on six principles: provide stakeholder value, holistic approach, dynamic governance system, governance distinct from management, tailored to enterprise needs, end-to-end governance system. Although the COBIT framework is a governance framework by origin, it contains a number of security elements.

Like the ISO/IEC 27000 series and the NIST Cyber Security Framework, COBIT 2019 provides a generic guidance for the implementation which needs to be adjusted for the specific enterprise. Like the NIST Cyber Security Framework, COBIT 2019 includes references to other frameworks which may be used for better understanding or alignment. However, this generic guidance is far less detailed than the ISO/IEC 27000 series and NIST Cyber Security Framework, almost requiring an enterprise to refer to other frameworks for details. Like the ISO/IEC 27000 series, COBIT 2019 uses a PDCA cycle.

"The CIS Critical Security Controls (CIS Controls) are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks" (Center for Internet Security, 2022). The CIS Controls contain 18 security controls, which can be seen in the appendix in table A4. Unique for the information security frameworks discussed so far is the distinction between three implementation

groups. These groups are separated based on the risk profile and resources for implementation of an enterprise. The first group, IG1, has been defined by as “essential cyber hygiene”, which is “the foundational set of cyber defense Safeguards that every enterprise should apply to guard against the most common attacks” (Center for Internet Security, 2022). The increase from one group to the next comes with an increase of safeguards needed to be implemented per security control. Each of these safeguards serves a different security function, such as Identify, Protect, Detect, Respond or Recover. Most safeguards also have a specific asset type to which they apply, like devices, applications, data, users or network.

The final framework discussed will be the Payment Card Industry Data Security Standard (PCI DSS). For businesses all over the globe accepting credit cards, compliance with PCI DSS is mandatory (PCI Security Standards Council, 2022). The PCI DSS are technical and operational requirements with the purpose of protecting cardholder data. The standard is based on six goals, which are represented by 12 requirements. These requirements are presented in table A5 in the appendix. The requirements can also be used for enterprises who do not deal with credit card information as a guideline to otherwise protect valuable information. PCI DSS uses a continuous process, like the PDCA cycle, namely an assess-repair-report cycle. In this cycle, an enterprise assesses the IT system and business processes for vulnerabilities, then repairs these vulnerabilities and finally documents and reports the repairs made to stakeholders. The PCI DSS requirements present a checklist of sub-requirements which have to be transformed into detailed checklists depending on the IT system and business processes of the enterprise. Such a checklist of sub-requirements could prove useful for businesses to get an overview as to how far their information security is before or during the implementation process.

2.2 Industry 4.0

Industry 4.0, or I4.0 for short, as it was coined by German researcher Wolfgang Wahlster (Szanja et al., 2020), is a strategic initiative introduced by the German government (Rojko, 2017). It contains nine pillars; big data, autonomous robots, simulation, additive manufacturing, Internet of Things, cloud computing, augmented reality, horizontal and vertical integration and cybersecurity (Erboz, 2017). Though the definition of the elements of Industry 4.0 differs per source, most will contain the aforementioned nine pillars or variants of those definitions (Culot et al., 2020).

According to Horváth & Szabó (2019), “the term “Industry 4.0” describes the increasing digitization of the entire supply chain”, which is especially relevant in the manufacturing industry. This increasing digitization would make it possible to “connect actors, objects and systems based on real-time data exchange.”

The implementation of Industry 4.0 technologies in SMEs has been quite limited, especially compared to the level of implementation in multinationals (Horváth & Szabó, 2019). This limitation is due to the higher barriers and lower driving forces for SMEs. “Researchers have pointed out that the lack of [a] skilled workforce and financial resources, standardization problems and cybersecurity issues may be particular problems” (Horváth & Szabó, 2019).

This thesis will focus on the three major technologies, Internet of Things, cloud infrastructure and big data (Deloitte Global analytics, 2020). Per technology, a number of elements will be discussed regarding information security. These elements will be discussed because similar questions are answered in the literature (Agarwal & Agarwal, 2011; Ahmed et al., 2017; Andrea et al., 2015; Kumar et al., 2018; Masood & Sonntag, 2020; Orzes et al., 2018) and because it provides the information needed for the creation of the framework.

- An explanation of the technology
- What barriers are there for implementation?
- Which changes are made during and after the implementation?
- How do these changes influence information security?

2.2.1 Internet of Things

“The Internet of Things (IoT) is an emerging global internet-based information architecture facilitating the exchange of goods and services” (Weber & Weber, 2010). The term “Internet of Things” was first coined by Kevin Ashton, then executive director of the Auto-ID Center, based on an RFID application (Madakam et al., 2015). Since then, many new technologies have been developed and deployed worldwide and “the visions for the Internet of Things have been further developed and extended” (Wortmann & Flüchter, 2015).

Simply stated, the Internet of Things is a network facilitating the connection between interrelated computing devices or other ‘things’ able to transfer data over a network without any form of human interaction. This does not mean that human interaction is not possible. A smart thermostat, for example, can be used as an interface to facilitate human interaction.

The Internet of Things can be described as a generic term containing multiple technologies able to be implemented in the network. Madakam et al. (2015) list some of the technologies: Radio Frequency Identification (RFID), Internet Protocol (IP), Electronic Product Code (EPC), barcode, Wireless Fidelity (Wi-Fi), Bluetooth, ZigBee, Near Field Communication (NFC), actuators, Wireless Sensor Networks (WSN), Artificial Intelligence (AI). Madakam et al. (2015) explain the last technology, AI, by saying that: “in an ambient intelligence world, devices work in concert to support people in

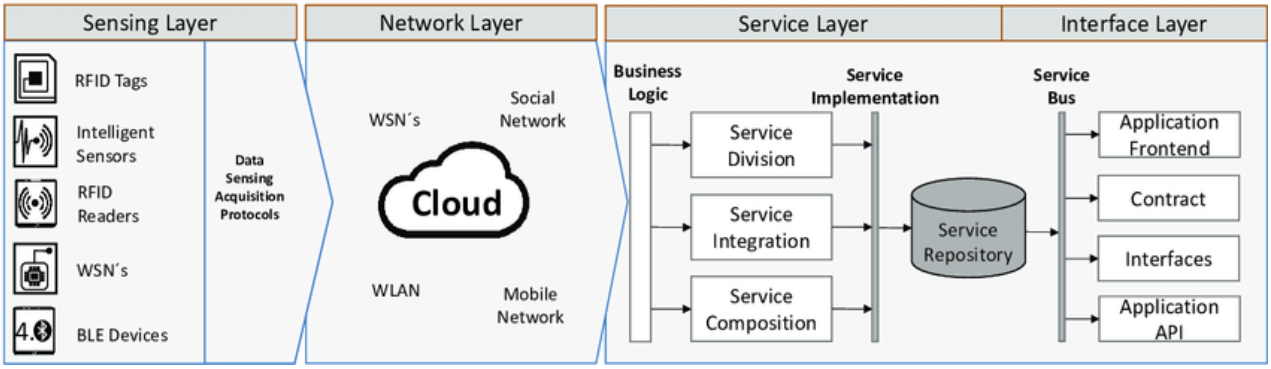
carrying out their everyday life activities in easy, natural way using Information and Intelligence that is hidden in the network connected devices." Referring back to the example of the smart thermostat, the system can decide whether to set the temperature to a certain number based on the situation. It may also be able to anticipate what the user wants from the system beforehand.

An Internet of Things architecture has, according to Li et al. (2015) and Nauman et al. (2020), four layers. These layers are interconnected but individual and can be maintained, upgraded and reused independently (Li et al., 2015). Each layer and its functionalities are as follows and are visually shown in figure 2:

- Sensing layer: integrated with hardware such as sensors and actuators.
- Network layer: infrastructure which supports the connectivity between the sensors and services.
- Service layer: creation and management of services needed for interfacing with users or applications. Includes data processing and data storage.
- Interface layer: interaction methods with users or applications, such as APIs and interfaces.

Figure 2

Service-oriented architecture for IoT.



Note. From Weiß et al. (2016, Figure 5), who adapted it from Li et al. (2015).

Because of the advancements in sensing and communication technologies, the possible applications of the sensors have increased over the years, increasing the number of sensors in different use-cases a company may use (Li et al., 2015). The size of the sensing layer will be different for every company, due to the number of sensors and actuators used. This size of the sensing layer has effect on the requirements of the network layer and service layer.

The network layer connects all things and lets them share data with other connected things. An incident with the network layer can compromise the availability of the information. This is also why the network layer must automatically discover and map things in a network, as undiscovered things are not capable of transferring information, limiting availability. Additionally, confidentiality of

information is also important in the network layer as information may not be shared with unauthorized people. Prevention of stolen data can be done using encryption of the data.

The service layer contains all of the service-oriented activities. These include information exchange, information storage, data management, ontologies database, search engines and communication (Li et al., 2015). Integrity of information is important in this layer due to the requirement to prevent corruption or loss of data and unauthorized modifications.

The interface layer provides a service which aids in the use of multiple incompatible devices. Li et al. (2015) illustrate the interface layer by comparing it with "Universal Plug and Play (UPnP), which specifies a protocol for the seamless interactions among heterogeneous things." In the interface layer, attention must be paid to the confidentiality of information. Authorizations of users must be correctly assigned, to prevent unauthorized users seeing the data.

Availability of the data is important in each of the layers for the same reason. If one of the layers becomes unavailable for any reason, the entire system may stop being available.

Madakam et al. (2015) state eight prerequisites for the successful implementation of Internet of Things. These prerequisites are:

- Dynamic resource demand
- Exponential growth of demand
- Availability of applications
- Real time needs
- Execution of the applications near to end users
- Data protection and user privacy
- Efficient power consumptions of applications
- Access to an open and interoperable cloud system

For this thesis, only the underlined prerequisites will be focused on during the creation of the framework as these are more in line with the main subject of this thesis. The other prerequisites are not relevant for information security, and are therefore not taken in to consideration.

Kamble et al. (2019, p. 157) present a list of adoption barriers for the implementation of Internet of Things. Most of the barriers are as expected with a new technology: lack of regulations, standards, (internet) infrastructure, human skill and validation. Relevant for this thesis is the barrier regarding security and privacy. Kamble et al. (2019, p. 157) say that: "Security is imperiled in the network-based system because of the threats like overwriting false data, accessing sensitive data and many other unauthorized intrusions which may paralyze the networks." Additionally, Kamble et al. (2019, p. 157) say that "RFIDs are more prone to these attacks" and that "issues related to encryption of data, internet connectivity, software protection, and authorization make the IoT system vulnerable to external security risks." All of the threats mentioned by Kamble et al. (2019) can be categorized into

the CIA triad, and the relevant threats and their preventative measures will be implemented in the framework.

Weber (2010) states that "IoT has an impact on the security and privacy of the involved stakeholders." Weber (2010) continues to state that "Private enterprises using IoT technology will have to include [the following] requirements into their risk management concept", referring to the following security and privacy requirements: resilience to attacks, data authentication, access control, and client privacy.

Resilience to attacks requires the system to avoid single points of failure and needs the system to adjust itself in the case of the failure of a part of the system, making it part of information availability. Data authentication is a part of information integrity. Access control is a part of information confidentiality. Client privacy is also a part of information confidentiality, as it regards the prevention of the client's information being available to anyone other than authorized users.

Necessary to mention is the coupling between IoT and SCADA (Supervisory Control And Data Acquisition) systems. "A SCADA system is a combination of hardware and software enabling the capture of data within, and automation of, industrial processes" (Metzger, 2021). These SCADA systems have been used since the 1960s for controlling industrial equipment, making it relevant for the manufacturing SMEs this thesis is directed to. The interaction between IoT and SCADA systems is limited to the functionalities which are added 'on top of' the SCADA system, but this does present further challenges as both systems need to be secure to prevent hacks or other forms of information security breaches (Datashield, n.d.).

2.2.2 Cloud Solutions

Also known as cloud computing or cloud services, cloud solutions are internet-based IT resources (del Vecchio, 2021; Joy, 2021; Red Hat, 2018; Suse, n.d.). As these IT resources are internet based, they are off the premises of the business requesting them, which will require different information security requirements. These security requirements will be discussed later. The IT resources can be requested on demand from cloud service providers. Unlike on-site IT resources, these cloud solutions are able to scale up or down quickly and on demand in order to meet business needs (del Vecchio, 2021; Joy, 2021; Suse, n.d.). This ability to meet demand is why using cloud solutions alongside an IoT implementation can be very valuable to the cloud user due to the flexibility of the cloud service and its cost.

Cloud solutions can be split into public clouds, private clouds and hybrid clouds (del Vecchio, 2021; Red Hat, 2018). A public cloud is a cloud which is partitioned into multiple parts, which are then distributed to multiple cloud-users. A private cloud is a cloud which is dedicated to a single user or

user group. The advantage over a public cloud is that the user has isolated access to the IT resources which are able to fully run behind the users' firewall (Red Hat, 2018). Finally, a hybrid cloud is either a mix of a private and public cloud, or a combination of multiple similar clouds. This configuration provides the possibility to move applications and data from a private cloud server to a public cloud server, or vice versa, depending on the needs. This can be done as a security consideration to, for example, only keep critical data in the private cloud.

Services being hosted on the cloud can also be split into three types. These types are IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). With each type of service, the cloud provider takes care of an increasing amount of work, as can be seen in table 4 below.

Table 4

Cloud service provider services.

On-site	IaaS	PaaS	SaaS
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Operating system	Operating system	Operating system	Operating system
Visualization	Visualization	Visualization	Visualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking
Legend:	Customer manages		Cloud service provider manages

Note. Adapted from Red Hat (2018).

With the use of cloud services, a different focus on information security needs to be made. Compared to having everything on-site, using cloud services makes the service provider responsible for most information security. However, not everything will be the responsibility of the cloud service provider, such as internal password security, i.e., having somebody else know your password, and wrong data entered into the system causing integrity failures. Additionally, Agarwal and Agarwal (2011) summarize six vulnerabilities to the confidentiality, integrity or availability of the information of the system it is contained in. These vulnerabilities are presented in table 5. Although only the underlined vulnerabilities are (partially) avoidable by users, users have to do all they can in order to ensure the confidentiality, integrity and availability of the information and/or the system is not lost due to their

preventable mistakes. Other measures, not only those mentioned in table 5, which need to be taken by the cloud service host to prevent this same loss will need to be addressed in the service level agreement (SLA) (Kandukuri et al., 2009). This will not only note the responsibility and accountability of the cloud service provider, but also give the user an overview of which measures are not taken care of. Another part which can be included in the SLA is monitoring of the cloud service provider. Elements like a required ISO/IEC 27001 certificate and/or a third-party assurance report are ways this can be solved. Such measures ensure that the information that is stored on the cloud servers is properly secured.

Table 5

Vulnerabilities to cloud service CIA.

Authentication: Risks appearing when users are able to enter accounts at a higher level and with more authorizations than was assigned to them due to unauthorized authentication, users may be able to access certain elements of the cloud services which they are not authorized to do.
Eavesdropping: The risk that an external, unauthorized party is able to monitor and intercept the flow of data between the users and the cloud service.
Denial of Service Attacks: The risk that an external party launches a denial-of-service attack (DoS) on the server or network of the cloud provider. This would result in the cloud servers becoming unavailable and prevents users from being able to interact with the cloud server.
Network Intrusion: Risks appearing when external parties are able to exploit security vulnerabilities within the software of the cloud service. This could enable the external party to access data of the cloud service users.
Inappropriate use of System Infrastructure: "The risk is that authorized users of a company's network may use the network for non-business uses such as inappropriate web browsing. This may result in litigation accusing employers and cloud service providers of employee harassment." (Agarwal & Agarwal, 2011, p. 258)
Session hijacking: Similar to eavesdropping, session hijacking is the risk that an external party is able to take over the connection between the client and server. This enables the external party to post as the original user, in turn giving the possibility to do everything the user is able to do.

Note. Adapted from Agarwal and Agarwal (2011). Underlined vulnerabilities are seen as (partially) preventable by users of the cloud service.

2.2.3 Big Data

Big Data refers to a dataset which is not able to be processed by traditional tools or methods (Humblot, 2021; Inukollu et al., 2014; Oracle, n.d.; SAS, n.d.). Big Data can also be described using the three V's; Volume, Velocity, Variety, which are all high/large when dealing with Big

Data (Humblot, 2021; Oracle, n.d.; SAS, n.d.). This means that the volume of data is large, the velocity (speed at which it needs to be handled) is high, and variety (different data formats) is large.

Ahmed et al. (2017) mention that "[...] the IoT is expected to produce a huge amount of data. The data generated from IoT devices can be used in finding potential research trends and investigating the impact of certain events or decisions." Therefore, when an organization decides to implement an IoT application, implementing Big Data is a logical step to take.

The lack of ability to process the data does not mean that the data is useless. On the contrary, the data can be used to gain new insights and knowledge of customers or processes. Oracle (n.d.) list seven benefits to be gained from the use of Big Data:

1. Product development;
2. Predictive maintenance
3. Customer experience;
4. Fraud prevention and compliance;
5. Machine learning;
6. Operational efficiency;
7. Stimulate innovation.

With the implementation of Big Data, a number of information security issues present themselves. This is especially the case when dealing with "sensitive information regarding customers and employees, as well as intellectual property, trade secrets and financial information" (Tankard, 2012). Additionally, having all the data centralized makes it a valuable target, making "it essential that Big Data stores are properly controlled and protected" (Tankard, 2012).

Even with the protection of Big Data being essential, businesses using Big Data "may not have the fundamental assets particularly from a security perspective" (Inukollu et al., 2014, p. 49). Furthermore, "If a security breach occurs to Big Data, it would result in even more serious legal repercussions and reputational damage than at present" (Inukollu et al., 2014, p. 49).

Inukollu et al. (2014) split the issues and challenges with Big Data into four levels: the network level, the authentication level, the data level and generic types. The network level are challenges related to network protocols and security, like distributed nodes and distributed data. The authentication level deals with encryption and decryption techniques, logging, and general authentication methods. The data level consists of challenges related to data integrity and availability. The last level, generic types, are challenges related to traditional security tools and security related to the use of other technologies.

Solutions for these challenges are presented by Inukollu et al. (2014) as follows:

Table 6

Solutions for Big Data challenges in the cloud.

File encryption	Network encryption
Logging	Software format and node maintenance
Nodes authentication	Rigorous system testing of map reduce jobs
Honeypot nodes	Layered framework for assuring cloud
Third party secure data publication to cloud	Access control

Note. The full explanation per solution can be found in the appendix in table A6.

Tankard (2012) states that access controls should be "granular enough to ensure that only those authorized to access data can do so". This is as a precaution to prevent sensitive information from being compromised. Additionally, access "controls should be set using the principle of least privilege" (Tankard, 2012). Continuous monitoring and active modifications when needed are also required to ensure effective access controls.

On the storage and encryption, Tankard (2012) says that "ensuring that data is archived as required and disposed of when no longer needed is another important security consideration", which reduces the risk of sensitive data being breached. Another method for reducing risk and making data unreadable is "encryption, tokenization and data masking, so that only those with the keys to unlock the data can do so" (Tankard, 2012). A final important requirement is having a legal department involved in the development of policies regarding the storage and disposal of data to be compliant with industry standards and government regulations.

3. Methodology

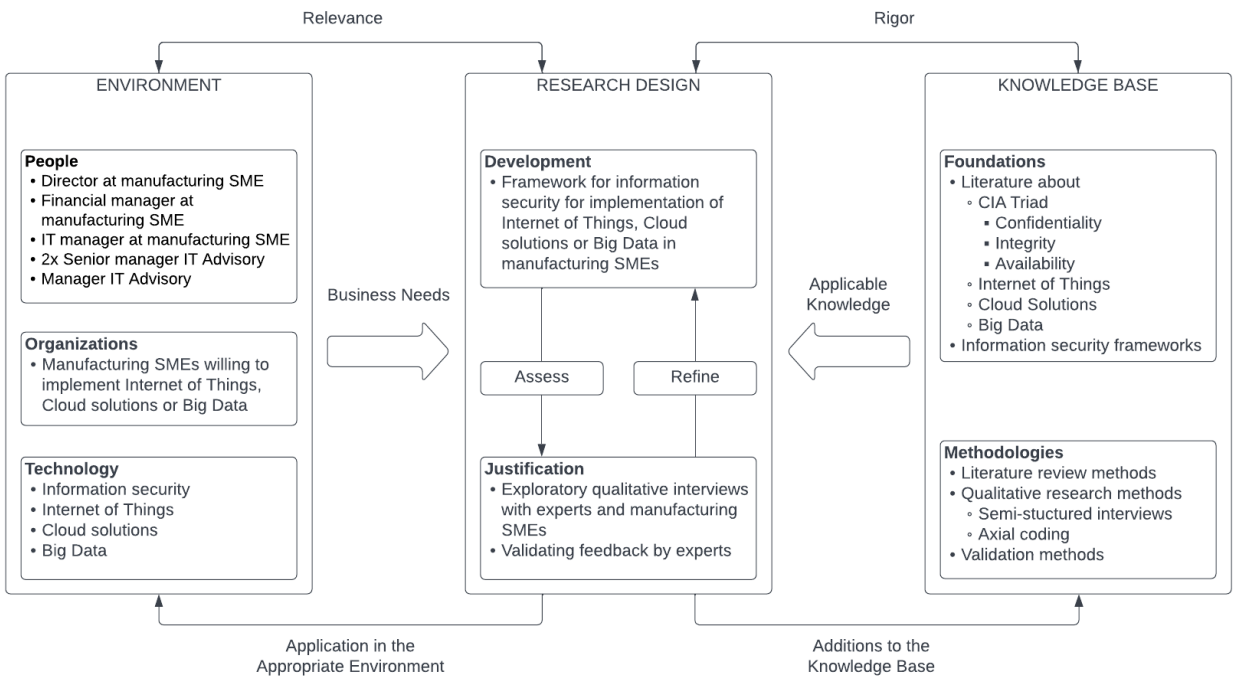
This chapter will present the research methods used during this thesis. Firstly, the research design will be presented. Following the research design, the methods for data collection for the primary and secondary data will be discussed. After this, the methods for the processing and analysis of the primary data are presented. Finally, the process of creation and validation of the proposed framework will be discussed.

3.1 Research Design

This thesis aims to develop a framework in the field of information management. For the research design, design science has been chosen. After consideration of a number of design science papers and frameworks by Peffers et al. (2007), Hevner et al. (2004), Wieringa (2014) and vom Brocke et al. (2020), a design science framework has been chosen. The information systems research framework by Hevner et al. (2004) was found to be the most fitting framework for this thesis. Therefore, this framework has been used to conduct this research. An applied version of the framework by Hevner et al. (2004) is depicted in figure 3 below.

Figure 3

Research design of this thesis according to Hevner et al. (2004).



Note. Adapted from Hevner et al. (2004).

For this thesis, a number of goals were set which must be achieved to be considered successful. These goals, which are also called design science criteria, are split into primary and secondary goals. Primary goals need to be achieved, whilst secondary goals are desirable, but not essential. The primary goals are:

1. The thesis must be sufficient to grant the author the degree of Master of Science in Information Management;
2. The created framework must be found applicable for actual use by experts;
3. Conclusions taken from this thesis are found to be additions to the current knowledge base in the field of information management;
4. The author gains new knowledge and skills in the field of information security.

Secondary goals are:

1. The interviewed manufacturing SMEs find the framework useful for (partial) implementation;
2. Baker Tilly, the business where the author enjoyed an internship find either the framework or conclusions useful for their business.

3.2 Primary Data

At the start of the research period, a number of meetings with Baker Tilly colleagues and thesis supervisor Joris Hulstijn were held to set and define the problem statement and scope of the research. This was done to set a scope relevant for both Baker Tilly and her customers, and the academic literature.

The primary qualitative data was collected through five semi-structured interviews. Two of these interviews were with customers of Baker Tilly and the other three interviews were with senior colleagues at Baker Tilly with a high level of expertise within the domain of information security. The overview of individuals which were interviewed can be found in table 7 below.

Table 7

Interviewed individuals.

Name	Function
Participant A	Director at a metalworking SME. (Company A)
Participant B	Financial manager at a metalworking SME. (Company A)
Participant C	IT manager at a metalworking SME. (Company B)
Participant D	Senior manager IT Advisory at Baker Tilly.
Participant E	Senior manager IT Advisory at Baker Tilly.

Participant F	Manager IT Advisory at Baker Tilly.

Note. Participant A and Participant B work at the same company and were not separately interviewed.

The interviewed customers of Baker Tilly were chosen on the criteria that they are active in the manufacturing industry. Other criteria such as company size or status of Industry 4.0 implementation were not considered, as this would possibly skew the results of the primary data collection.

Colleagues at Baker Tilly who were interviewed were chosen based on seniority and experience with customers trying to implement or successfully implemented Industry 4.0 technologies.

The semi-structured interviews were held between the 19th and 30th of April through Microsoft Teams. All interviews were recorded with permission and were consequently processed, which will be discussed in chapter 3.4.

During the interviews with customers, questions about the current implementation of Industry 4.0 technologies and information security were asked. Depending on whether any technologies were implemented, questions about this implementation, the current information security and use of any information security frameworks were asked. This was done separately for the three technologies discussed in this thesis, namely Internet of Things, cloud solutions and Big Data. In the case a technology was not implemented but plans were made, questions regarding these plans and specifically the use of information security frameworks were asked. If the customer had no intention of implementing a specific technology, this technology would be ignored for the questions regarding information security.

In the interviews with the customers of Baker Tilly the concept of the CIA Triad was not directly discussed, as their knowledge and the practical use of this concept within the company was expected to not be sufficient for the interview. However, the concepts which are contained within the CIA Triad, i.e., elements of confidentiality, were discussed.

The questions prepared for the semi-structured interviews can be found in tables A7 and A8.

3.3 Secondary Data

For the literature review, 81 papers and other sources were found and used. This search started by looking for broad subjects like “Industry 4.0”, “information security” and “CIA Triad”. After this search and research more intricate subjects like “confidentiality in cloud solutions” and “Internet of Things architecture” were looked for. This enabled the search for more specific papers and other sources depending on the need within the literature review.

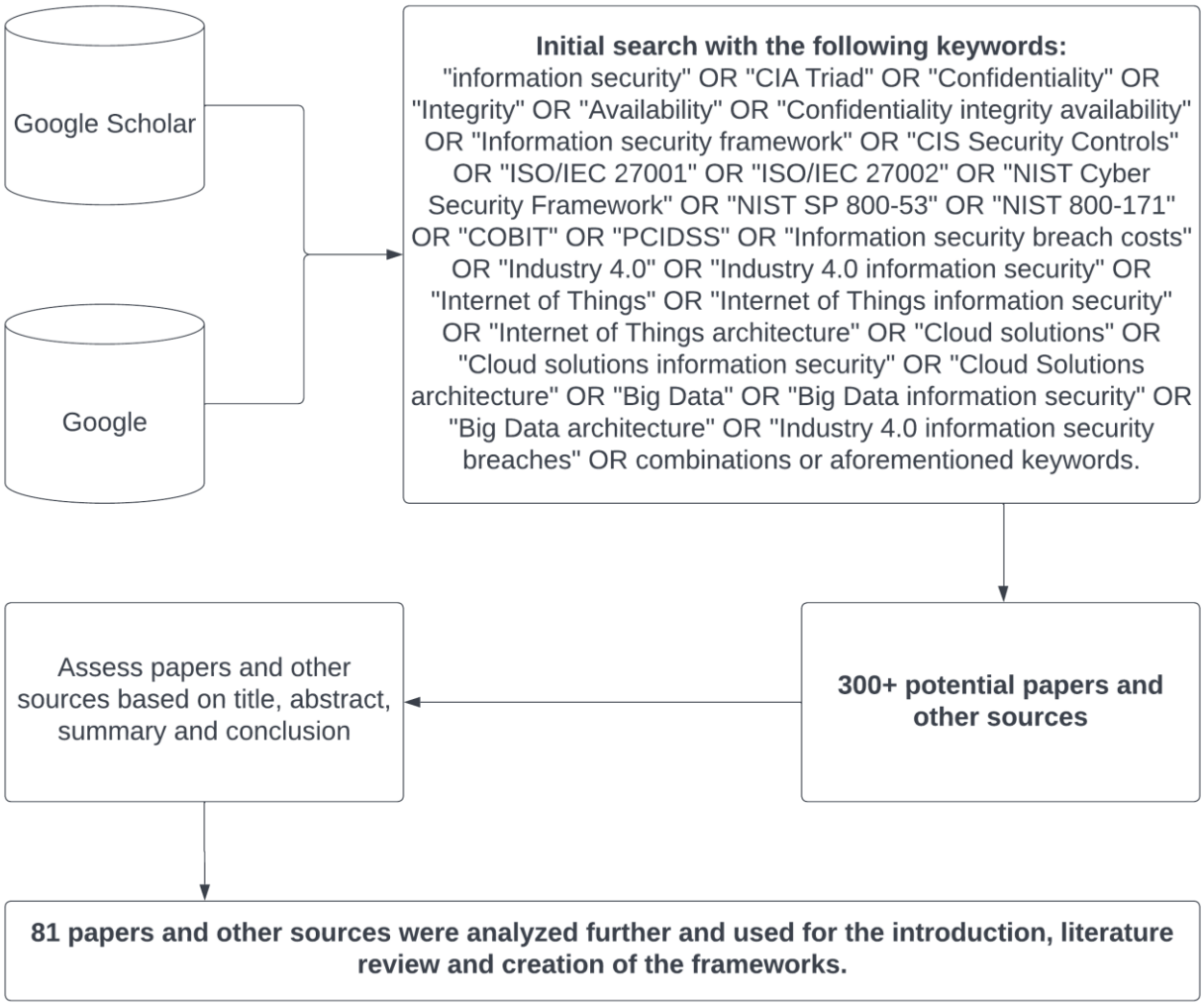
All papers were sourced through Google Scholar, either through direct search or references in other papers. All other sources were found through a normal Google search.

If a source was deemed relevant, based on the title, abstract and conclusion, the paper, or parts of the paper were read and used. The information security frameworks were found by searching for general terms, but also through references in sources used for parts of the literature review.

The process of sourcing this literature is shown in figure 4 below.

Figure 4

Process of sourcing and analyzing papers and other sources.



3.4 Method of Data Analysis

The qualitative data received from the interviews was analyzed using the axial coding method, as described by Williams & Moser (2019). This method has the goal that “collected data can be sifted, refined, and categorized with the goal of creating distinct thematic categories” (Williams & Mozer,

2019). To do this, “researchers need to engage in continuous analysis, cross referencing, and refining theme categorization.” (Williams & Mozer, 2019).

In order to perform axial coding, the previous step, open coding, must be completed. Open coding is done by sifting through the responses in the interview and organizing “similar words and phrases, concept-indicators, in broad initial thematic domains” (Williams & Mozer, 2019). Then, in axial coding, the relations in the broad thematic domains are identified and developed into related core codes.

For this process, the constant comparison method, as described by Williams & Mozer (2019), combined with a four-step process as described by Delve (2022) was used. The constant comparison method is a data organizing and refining activity. The focus of the constant comparison method “is to compare continually [*sic*] data collected, emergent themes, and their coding in order to continually create, refine and newly create categories” (Williams & Mozer, 2019).

The four-step process of completing axial coding as described by Delve (2022) is as follows:

Table 8

Method for axial coding, as described by Delve (2022).

1. Turn your data into small, discrete components of data; a. In this step, the qualitative data, which in this case are the interviews, are split into shorter pieces. The size of these pieces was chosen to be sentences.
2. Code each discrete pieces of data with a descriptive label; a. Each sentence is to be interpreted and labeled based on the subject and property of the sentence. b. During this, the labels placed on groups of sentences with a similar subject should be the same.
3. Find connections and relationships between code; a. Analyze the labels placed on the sentences and identify connections between them. These connections can, for example, be causal, contextual or consequential.
4. Aggregate and condense codes into broader categories. a. Create new, broad categories to label the groups of sentences which are found to be connected in step 3. Assign these new labels to the sentences.

Note. Adapted from Delve (2022).

This process was done according to the four steps seen above, except for step 4, which was done earlier by the creation of a list of broader categories based on the subjects in this thesis. These broader categories were then used in step 2.

3.5 Framework Creation

The framework will be created from three sources. The first source are the interviews with the customers of Baker Tilly and the senior colleagues at Baker Tilly. The second source is the literature as described in chapters 2.1 and 2.2. The literature study contains threats and measures which will be considered for the framework. The third source are the information security measures as described in chapter 5.2, which contains a baseline and best practices for information security based on the information security frameworks discussed in chapter 2.1.4. This third source, which can be found in tables 9 and 10, was created by going through the information security frameworks and looking for measures relating to the different parts of the CIA Triad. The three sources will all be used to find threats, risks and security measures corresponding to the categorization of the CIA Triad.

Due to the, by the authors opinion, clear and user-friendly documentation of the measures and their explanations, the CIS Security Controls will be used for the main source for the new framework which is created in this thesis. This means that where a measure was seen as fit for the baseline, as described in table 10, it was taken from the CIS Security Controls. If the CIS Security Controls did not contain the measure, other frameworks and literature were referenced for the creation of the measure. Table 11 contains a note to provide the original source of the measure and its explanation.

The framework will be split into three parts; a baseline of best practices in information security measures, baseline measures for each of the Industry 4.0 technologies discussed and an overview of different cloud services and the distribution of the relevant responsibilities. The baseline of best practices is an overview of all the measures. Additionally, the measures will be split into measures for confidentiality, integrity and availability of information. This will give businesses the opportunity to learn where certain measures provide value, and it gives a clear overview to which parts of the information are made more secure through each measure. Furthermore, in case the business wants to add additional information security measures, these can be found by looking for measures increasing either the confidentiality, integrity or availability of the information. Table 11 will reference to this overview of best practices to split the measures in to groups which are relevant for the specific technology, and the levels or layers within.

3.6 Framework Validation

The initial version of the framework was sent to the interviewed senior colleagues at Baker Tilly. Along with the framework, a number of questions and discussion points are added, which are requested to be answered. Firstly, the respondents are asked whether the framework contains all (and more) measures they expected it to contain, and if there are any more measures which they miss.

Secondly, they are asked whether the explanation of each measure is sufficient to understand and implement. Thirdly, they are asked if they deem the framework usable for (other) SMEs in the manufacturing industry, which would test the generalizability of the framework. Finally, additional room for other remarks is available. The initial version of the framework was also sent to the interviewed businesses, but these were not asked for feedback. This will also be addressed again in chapter 5.6.

Based on the feedback received from the respondents, a revised framework is made. This revised framework will be featured in chapters 5.3, 5.4 and 5.5. The initial framework as it was before the feedback will be available in the appendix, with annotations indicating where elements were changed. The revised framework will finally be sent to all interviewed parties as confirmation that the feedback which was received was actually used.

4. Data Analysis

This chapter discusses the analysis of the primary data, according to the method explained in chapter 3.4. The most relevant parts of the 5 interviews will be discussed in this chapter. Whether a part was relevant was based on whether it was in line with the subject of this thesis.

4.1 Need for Industry 4.0

Participant F is of the opinion that "the number of IT staff members is not decisive for the willingness to implement new technologies. This more often comes from the directors, production staff or specially assigned innovation staff". Participant D mentioned that in businesses, "the number of workers is dropping, whilst machines and sensors are ever increasing."

According to the interviewed participants, the level of implementation of Industry 4.0 technologies is wildly different between companies. Participant E mentioned that "the movement of SMEs to the cloud is happening, as those services keep becoming more professional. Cloud is also more flexible when wanting to work remotely". On the other hand, participant F mentioned that "SMEs are just orientating for the implementation of cloud services, but production SMEs are more traditional, and often family businesses. These family businesses often have the servers on-premises, as the production is not allowed to come to a halt due to loss of internet connection".

Another reason why production SMEs are not quickly adapting cloud solutions is, according to participant F, that "production systems are not suited for the cloud due to the older systems and backlog of updates. Additionally, the time it takes for the costs to be repaid is too long, when innovating the systems to be able to work on the cloud. This results in older, often less critical, systems still being operational for a long amount of time".

Participant F mentioned that in his knowledge "Big Data is implemented limitedly in manufacturing SMEs." Participant E, who had some experience with Big Data in general, mentioned that "for Big Data, reproducibility is necessary. Additionally, the quality and integrity of data need to be very high. Integrity can be improved by coupling the data to an external source." Participant D mentioned that in the healthcare sector, this is already done, as sometimes a group of healthcare businesses combine their data in order to gain proper insights from Big Data. Finally, participant E finds that "at the start of a Big Data process, research needs to be done to the possible negative effects possibly emerging from the results."

4.1.1 Industry 4.0 in businesses

About business B, participant C mentioned that “IoT is only used as an exception for customers. Production equipment is manually operated and not connected to the internet.” Additionally, participant C mentioned that “within the business, there is no vision for new technologies, because it is currently not necessary. Projects for customers are often disconnected from the internet on purpose.” This removes the need for business B to gain expertise in IoT.

For cloud solutions, participant C mentioned that “cloud is implemented for new applications or applications which are easily adjusted to be usable in the cloud. This is done because it makes the connection with other systems easier.” Finally, Big Data is not used in business B, as, according to participant C, “there is no vision for it from the directors. The support for it would be available from the IT department.”

In business A, a customer portal is used to receive orders according to a data standard, SCSN. Participant A claimed that “the customer portal makes the order ready for automatic production. The complete automatic production is not fully finished and implemented, but from order to ready for packaging is working.” This indicates a high level of IoT implementation.

4.2 Current Information security

According to participant D, whose expertise lies within the healthcare sector, where IoT, cloud solutions and Big Data are either upcoming or already implemented, “the technologies have already proven themselves in the healthcare sector, the implementation of them can go very fast, but information security is often forgotten. The vision for the new technologies in the healthcare sector matches that of the manufacturing industry, which provides the opportunity to compare experiences and problems. Participant D concludes that ”this lack of attention to information security is also found in other SMEs, as the feeling for necessity of information security is missing with many SMEs. When machines are running, not much is done to them, as this could bring risks to the environment. The search for improvements can already be found risky, let alone implementing these improvements. What is running fine is often let alone to do its thing.” On the other hand, according to participant F, “the management [of the three businesses discussed] recognizes that good IT and information security provide a competitive advantage and result in cost savings.”

4.2.1 On-premise Servers

For businesses who have their servers on-premise, participant E mentioned that “on-premise has the advantage that it is less accessible by outsiders, as the connection [and therefore data] does not have to traverse the internet. The question is whether the average SME can withstand the threats coming

towards on-premise servers. This can also be wishful thinking and SMEs need more expertise if they want to keep on-premise servers." Participant F has a similar conclusion, with an example where "the company has all their servers strategically on-premise, because they think they are better equipped to protect and manage the servers."

4.2.2 Intuition Versus Framework

This phenomenon of keeping servers on-premise, combined with the, as participant F mentioned, "lack of use of ISO/IEC 27001 by production businesses" can come from the wishful thinking participant E mentioned. Furthermore, according to participant F, "information security at SMEs was more often than not based on intuition, which could have some common ground with frameworks." According to participant E, "smaller companies work with frameworks even less often. If they try to use them, most times a number of parts are missing or incomplete. The frameworks can be so large that somebody with knowledge is needed."

For business A, participant A and B mentioned that "no information security framework is used, but advice from a partner was used to implement honeypots and segment the network into seven WLANs." Regarding an estimation of risk versus damages, participant A also mentioned that "we try to delay problems from occurring, as we try to keep the security as good as we can. We aim to be better protected than the neighbor, which still is not perfect, but we try without it costing too much."

4.2.3 Costs and Risks

Regarding costs, participant F says that "the biggest blockade is money, information security costs money, but does not directly return anything. Every investment will be double, triple checked and management will most times only actually do something when an incident has happened to them or others nearby." Participant A mentioned that "managers who don't know what the risks can be, will more quickly waive the threat away and spend less or no money on information security." Participant A also questioned whether a business should be "willing to spend more money now, to repel an attack later. SMEs are in the same playing field as multinationals, which have a lot more to spend to repel attacks."

A risk of insufficient information security is, according to participant D "sensors falling into the wrong hands. Especially with machines that can be physically dangerous. Critical systems are running on old software more and more often." Additionally, multiple participants have noted that not many businesses have a separate testing environment. Participant F also mentioned that "manufacturing SMEs often have less privacy sensitive information; this makes the priority of protecting information less. The more important factor is availability of the process, keeping production going is more important than losing data."

4.3 Use of Other Frameworks by SMEs

Participant D mentioned that in Dutch healthcare, the NEN 7510 is a mandatory information security framework. But even this mandatory framework "gives no demands for IoT implementation, causing businesses to struggle with the information security for it. This results in them leaning on the advice and support of suppliers. They struggle with implementing other frameworks for the missing piece too."

For cloud solutions, multiple participants mentioned that manufacturing SMEs do little monitoring. Participant C says that "we don't monitor our cloud providers. We do want them to have an ISO/IEC 27001 and we sign a processing agreement, but that is it." Participant E personally finds "the ISO/IEC 27001 is too weak on its own. A minimal addition is addressing expectations to the cloud provider and an independent firm to test this. But this is not a case of 'one size fits all', expectations can be different." Participant D also finds that "expectations of cloud providers are not concrete enough in current frameworks. They only state that certain elements need to be present, not how they should be addressed."

Participant C claims that to his knowledge "customers have no demands for a certain level of information security. We do not have an ISO/IEC 27001 certificate and we do not need one. We do try to work according to those frameworks."

4.4 Requirements of Framework

The participants had a number of requirements they wanted to see in the framework which was developed in this thesis. Some are already mentioned before in this chapter.

R1. Requirements to cloud providers should contain at least:
    a) An ISO/IEC 27001 certification;
    b) Expectations of the business to the cloud provider;
    c) An independent third party controlling these expectations and requirements.
R2. The framework has to explain when to implement it and for which type of manufacturing SME.
R3. Somebody without experience (but with some IT knowledge) should be able to implement it. We want to avoid hiring consultants to implement something.
R4. Change management, logical access and patch management should be covered.
R5. The framework should be an entry-level framework, containing the baseline for information security.

5. Framework

In this chapter, the framework which has been made is presented. In addition to this, an overview of the current situation of information security for IoT, cloud solutions and Big Data in other, already existing frameworks is given. This overview will discuss whether any missing measures, incomplete measures, and/or measures where change is needed are present in the current frameworks. Following this, an analysis of the frameworks discussed in chapter 2.1.4 based on the CIA Triad, as discussed in chapter 2.1.1 is made. That analysis will then directly be used for the creation of the framework, which can be found in chapter 5.5, with a graphical overview of the framework before that, in chapter 5.3, and an explanation of how to use the framework in chapter 5.4. Finally, an overview of the verification steps taken will be shown in chapter 5.6. This will contain the feedback which was given by senior colleagues at Baker Tilly and the interviewed customers of Baker Tilly, along with the measures taken to process this feedback. The original framework, as it was before the feedback can be seen in the appendix in table A9.

5.1 Current Situation

Currently, the frameworks which were analyzed and discussed in chapter 2.1.4 are a collection of generic measures which do not provide a baseline, with the exception of CIS Security Controls, and are not focused on a specific technology or business type. The exception for CIS Security Controls is due to the differentiation into three implementation group levels, of which the lowest level can be seen as a baseline of generic information security measures.

The lack of a baseline and overview of measures needed for minimal sufficient information security make these frameworks difficult to categorize into relevant measures and implement when wanting to implement an information security baseline. A business without an employee with knowledge about information security has a number of options they may take to be able to implement an information security baseline, which each have a downside.

1. The business may need to contact a third party to provide the relevant information security measures, but this may prove too expensive for an SME with limited budget.
2. The business may implement a number of measures based on own predictions, knowledge or research, which can prove to be an insufficient or incorrect selection of measures.
3. The business may try to implement all measures found in a framework, which can go over budget and/or be insufficiently implemented due to budget-constraints.

Each one of these options can result in inadequate information security, resulting in all types of threats being able to inflict harm to the systems and data within, resulting in harm to the business.

In the case the business has an employee with knowledge about information security, the points mentioned before may not apply, but from the interviews it was concluded that this does not happen often in manufacturing SMEs.

The lack of focus on a specific technology and business type can also follow the same options for solutions and the same conclusion. The measures will be too generic and some measures will even be irrelevant.

Due to this, the framework which is created in this thesis will need to address and include the following:

1. The measures will need to provide a baseline for sufficient information security, without needing to categorize the measures.
2. The framework needs to categorize the measures into the different elements of specific technologies. In this case, the technologies are IoT, cloud solutions and Big Data.
3. The framework needs to be focused on a specific business type. In this case, the business type is manufacturing SMEs.

A framework which already addresses one of the aforementioned requirements is the CIS Security Controls. Due to the, by the authors opinion, clear and user-friendly documentation of the measures and their explanations, the CIS Security Controls will be used for the main source for the new framework which is created in this thesis.

5.2 Information Security Measures

In this chapter the parts of the existing frameworks as discussed in chapter 2.1.4 will be analyzed and reconfigured to fit the CIA Triad. This is in order to gain a baseline and overview of best practices for each of the elements in the CIA Triad. Parts of the existing frameworks which cannot be refitted will be omitted for the creation of the new framework in this thesis. This is done because to keep all the measures relevant to the CIA Triad.

Other tenets, as discussed in chapter 2.1.1 and shown in table 1, and as described by Samonas and Coss (2014) are also analyzed. These additional tenets are underlined and can refer to other measures which encompass its definition or part of it.

Some parts of the existing frameworks are split into specific codes, which can be referenced back to the main measure as it is found in the appendix.

First, in table 9, the additional tenets which fall into multiple parts of the CIA Triad will be split to make its elements fit a single part of the CIA Triad. These elements are then added to the appropriate

part of the CIA Triad and are underlined in table 10. After this it will be noted whether that element is already analyzed or not. If not, the existing frameworks will be reconfigured to also fit that element.

Table 9

Tenets split into single CIA Triad elements.

Confidentiality and Integrity	**Split into parts**
1. Trust (Authorization and password protection)	1. Authorization – part of Integrity 2. Password protection – part of Confidentiality
Integrity and Availability	
1. Correctness in specification (System is fit for its purpose, access removal control)	1. Access removal control – part of Availability 2. System is fit for its purpose – part of Integrity
Confidentiality, Integrity and Availability	
1. Identity management (management of personal identifying data, the right entities have to use the right resources (data, applications) when they need to, without interference, using the devices they want to use.)	1. Authenticity – part of Integrity 2. Authorization – part of Integrity 3. Password management – part of Confidentiality 4. Devices on the network – part of Availability 5. Working locations – part of Availability 6. Audit log – part of Integrity 7. SSO – part of Confidentiality

Table 10 contains the CIA Triad, split into its relevant parts, as discussed in chapter 2.1.1. and its subchapters.

Table 10

Existing frameworks reconfigured in to the CIA Triad.

Confidentiality	**Reference to existing frameworks**
1. Access control (Password protection and password management)	ISO/IEC: A9.2.4, A9.3, A9.4.2, A9.4.3 NIST: PR.AC-7, PR.AT CIS: Controls 4.7, 5, 6, 14.3 PCI DSS: Requirements 2 and 8
2. Encryption (Encryption of data in storage and transit.)	ISO/IEC A10, A13.2, A14.1.3, A15 NIST: PR.DS-1, PR.DS-2, PR.DS-5, PR.PT-4 CIS: Controls 3, 14.4, 14.5, 15.4, 16.11 PCI DSS: Requirements 3 and 4
3. Password protection/ password management (Accounts are protected by passwords)	Addressed in Confidentiality 1: Are you who you say you are?

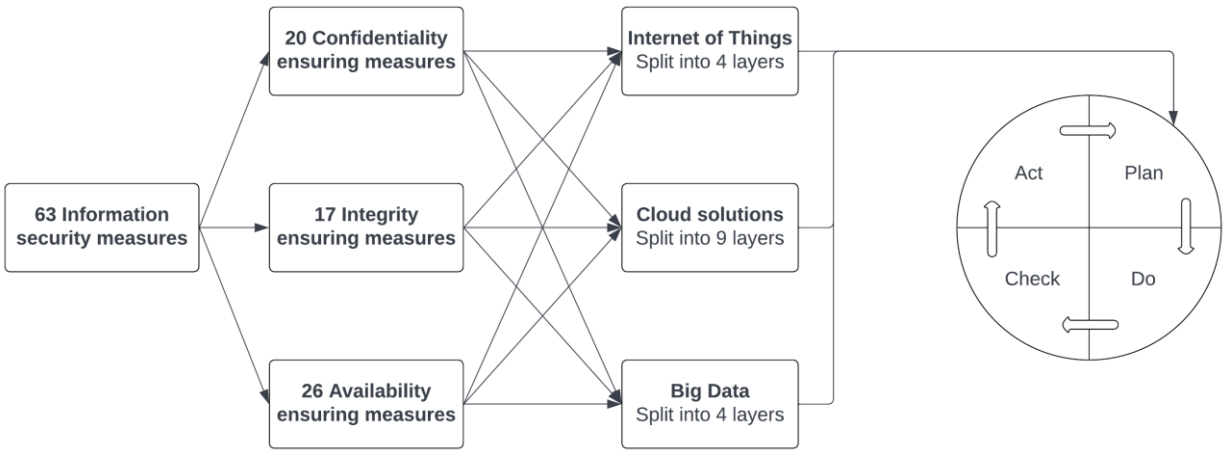
4. SSO (Ability to sign in to multiple applications using a single (strong) password)	Addressed in Confidentiality 1: Are you who you say you are?
Integrity	
1. Security control (Authorization of users.)	ISO/IEC: A6.1.1, A9 NIST: PR.AC CIS: Controls 3.3, 6 PCI DSS: Requirements 7, 8 and 9
2. Concurrency control (Prevention of inconsistencies due to concurrent access of multiple users.)	Not directly referenced in any frameworks
3. Reliability control (Prevention of hardware or software malfunctions.)	ISO/IEC: A11.2.4, A12.2.1, A12.3.1, A12.5.1, A14.2.3, 14.2.4 NIST: PR.DS-6, PR.DS-8, PR.IP-4, DE.AE-1 CIS: Controls 4 PCI DSS: None
4. Integrity control (Prevention of semantic errors made by users due to carelessness or lack of knowledge.)	ISO/IEC: A6.1.1, A7.2, A12.2.1 NIST: PR.AT, DE.DP-1 CIS: Controls 14 PCI DSS: None
5. Authenticity (Digital signature, valid and associated to a person)	Not directly referenced in any frameworks
6. Non-repudiation (Digital signature, not deniable)	Not directly referenced in any frameworks
7. Responsibility (Formal and informal, contract and not in contract)	Addressed in Integrity 4: Integrity control
8. Integrity of people (Live according to values, honest)	Not directly referenced in any frameworks
9. Ethicality (Right behavior)	Not directly referenced in any frameworks
10. Authorization (Authorization of users)	Addressed in Integrity 1: Security control
11. System is fit for purpose (Data and authentication are processed as designed)	Addressed in Integrity 3: Reliability control
12. Audit log (Log of login attempts)	ISO/IEC: A12.4 NIST: PR.AC-1, PR.PT-1 CIS: Controls 8, 16.11 PCI DSS: None
Availability	

1. Maintenance of software and hardware (updating, repairing and optimizing server, network or storage hardware).	ISO/IEC: A8.1.1, A11 NIST: ID.AM-1, ID.AM-2, PR.MA CIS: Controls 2, 12.1, 14.7 PCI DSS: 6
2. Maintenance of technical infrastructure (physical data traffic infrastructure, cooling, power supplies).	ISO/IEC: A11.2 NIST: ID.AM-1, PR.AC-2, PR.DS-4, PR.MA, DE.CM-7 CIS: 4.2 PCI DSS: None
3. Disaster recovery plan (sudden partial or complete loss of data is repaired as soon as possible).	ISO/IEC: A6.1.3, A16.1.1, A16.1.2, A16.1.5 NIST: RS.RP, RS.CO-1, RS.CO-2, RC.RP CIS: Controls 11, 15.4, 17 PCI DSS: None
4. Access removal controls (Account lockout)	ISO/IEC: A9.3.1, A9.4.2, A11.2.8, A11.2.9 NIST: None CIS: Controls 4.3, 4.10, 4.11 PCI DSS: None
5. Devices on the network (List of devices authorized to access the network)	ISO/IEC: None NIST: ID.AM-1 CIS: Controls 1, 4.12 PCI DSS: None
6. Working locations (List of locations and networks from which the network can be accessed)	ISO/IEC: NIST: None CIS: Controls 6.4 PCI DSS: None

5.3 Overview of Framework

Figure 4

Overview of information security framework for Internet of Things, cloud solutions and Big Data implementation.



5.4 Use of Framework by SMEs

The use of the framework is as follows:

1. Read the introduction, the measures and the explanations of the technologies.
2. Decide which technology to implement, and gather the relevant information security measures.
3. If needed, adjust the measures according to the situation the business is in.
4. Implement the measures in the business.
5. Check the effectiveness of the measures by self-assessments, external audits or pen-tests.
6. Depending on the results of the effectiveness check, adjust the information security measures.
7. Return to step 4.

5.5 Framework

This is a baseline information security framework created with the focus on the implementation of Internet of Things, cloud solutions and Big Data. The targeted businesses for which this framework is created are SMEs in the manufacturing industry with the ambition of implementing Internet of Things, cloud solutions and/or Big Data.

This framework consists of 63 measures, each addressing an element of information security based on the so called ‘CIA Triad’. This CIA Triad consists of confidentiality, integrity and availability.

5.5.1 CIA Triad

The first part of the CIA Triad, confidentiality, concerns itself with the protection of sensitive information. Meaning that in every scenario, information is secure and only accessible to individuals who are authorized to do so.

The second part of the CIA Triad, integrity, concerns itself with maintaining the consistency, trustworthiness and accuracy of data over its entire lifecycle.

The third and final part of the CIA Triad, availability, deals with the guarantee that there is consistent access to all information according to specifications.

Each one of these parts are split into further aspects which contain a number of measures which together ensure the control of those aspects.

5.5.2 Technologies

The framework is created with the focus on the implementation of Internet of Things, cloud solutions and Big Data. Each of these technologies are explained below.

Internet of things can be described as a network facilitating the connection between interrelated computing devices or other ‘things’ able to transfer data over a network without any form of human interaction. This does not mean that human interaction is not possible. A smart thermostat, for example, can be used as an interface to facilitate human interaction. The measures for the Internet of Things are split into four layers; sensing layer, network layer, service layer and interface layer. Each of these are briefly explained in table 12.

Also known as cloud computing or cloud services, cloud solutions are internet-based IT resources. The IT resources can be requested on demand from cloud service providers. Unlike on-site IT resources, these cloud solutions are able to scale up or down quickly and on demand in order to meet business needs. This ability to meet demand is why using cloud services alongside an IoT implementation can be very valuable to the cloud user due to the flexibility of the cloud service and its cost. This is why this framework recommends the use of cloud services when implementing an IoT system. Depending on if the business uses an IaaS, PaaS or SaaS cloud service, different elements will need to be managed by the business. This can also be seen in table 13.

Furthermore, cloud solutions can be split into public clouds, private clouds and hybrid clouds. A public cloud is a cloud which is partitioned into multiple parts, which are then distributed to multiple cloud-users. A private cloud is a cloud which is dedicated to a single user or user group. Finally, a hybrid cloud is either a mix of a private and public cloud, or a combination of multiple similar clouds. This configuration provides the possibility to move applications and data from a private cloud server to a public cloud server, or vice versa, depending on the needs. This can be done as a security consideration to, for example, only keep critical data in the private cloud.

For the implementation of cloud solutions, the measures are split according to the specifications in table 13. Depending on the type of service (IaaS, PaaS, SaaS), measures will either need to be implemented by the business directly, or be implemented by the service provider. In the case the service provider needs to implement the measures, a service level agreement (SLA) will need to be formulated containing the security requirements of the business based on the appropriate measures. The business will then have to (in)directly assess that these measures are actually implemented correctly, as described in measure 37.

For the use of a public, private or hybrid cloud service environment, there are no differences in this framework. Depending on the sensitivity of data and type of cloud environment, the relevant measures may be differently implemented. For example, a public cloud service environment may be assessed more on privacy towards other users of the same cloud server than a private cloud, which is dedicated solely towards a single business.

An example in which certain data is only allowed on a specific cloud server is when dealing with privacy laws. It is, in those cases, not always allowed to store the data in every country.

Big Data refers to a dataset which is not able to be processed by traditional tools or methods. Big Data can also be described using the three V's; Volume, Velocity, Variety, which are all high/large when dealing with Big Data. This means that the volume of data is large, the velocity (speed at which it needs to be handled) is high, and variety (different data formats) is large.

5.5.3 Usage of the Framework

Table 11 contains the measures extracted from the existing information security frameworks, based on literature and interviews. Each measure is explained, is given a number and is categorized with a number of similar measures.

In table 12, an overview of the elements of the Internet of Things, cloud services and Big Data are shown, together with an explanation for that element, and it's appropriate important/ relevant measures. These measures can directly be referenced back to the first table using the numbers.

The measures describe a goal which needs to be achieved business or business layer wide. As every business is different, the measures may need to be slightly adapted to fit the applications, servers or users. Some measures have examples of implementations added, which give the business advice to the practical implementation of the measure.

The measures are described in a way most people interacting with IT are able to understand them, without needing to be tech-savvy.

The implementation of the measures in this framework will need to be done using a PDCA-cycle. A PDCA-cycle stands for: plan, do, check, act. As this cycle is also a part of an ISMS (Information Security Management System), this is relevant for any business wanting to also use an ISMS. Each of the parts can be described as follows (VNG, 2021):

- Plan: the information security policy and measures are chosen.
- Do: the information security measures are executed.
- Check: the effectivity of the information security measures is measured. This can be done with self-assessments, external audits or pen-tests.
- Act: any risks found in the 'check' phase are evaluated and information security measures are adjusted accordingly.

As the name suggests, after the 'act' phase, go back and continue with the 'plan' phase.

For certain measures, such as the measures concerning encryption, it is not defined which standard is advised or required. In these cases, the users of the framework are advised to search for the current standards. This can be done through contact with machine suppliers, the ISO/IEC, DAMA, or an internet search for other guidelines. Due to the continuing changes in standards, a list of standards to be used is not provided, as this may quickly be outdated and therefore can provide inadequate advice.

5.5.4 Information Security Risks

A number of risks and barriers become prevalent when implementing IoT, cloud solutions and Big Data. Most of the barriers are as expected with a new technology: lack of regulations, standards, (internet) infrastructure, human skill and validation. But with every technology, a number of risks need to be mitigated.

For IoT, Kamble et al. (2019, p. 157) say that: "Security is imperiled in the network-based system because of the threats like overwriting false data, accessing sensitive data and many other unauthorized intrusions which may paralyze the networks." Additionally, Kamble et al. (2019, p. 157) say that "RFIDs are more prone to these attacks" and that "issues related to encryption of data, internet connectivity, software protection, and authorization make the IoT system vulnerable to external security risks."

For cloud solutions, the risks are more centered towards network issues, such as:

Authentication: Risks appearing when users are able to enter accounts at a higher level and with more authorizations than was assigned to them due to unauthorized authentication, users may be able to access certain elements of the cloud services which they are not authorized to do.
Eavesdropping: The risk that an external, unauthorized party is able to monitor and intercept the flow of data between the users and the cloud service.
Denial of Service Attacks: The risk that an external party launches a denial-of-service attack (DoS) on the server or network of the cloud provider. This would result in the cloud servers becoming unavailable and prevents users from being able to interact with the cloud server.
Network Intrusion: Risks appearing when external parties are able to exploit security vulnerabilities within the software of the cloud service. This could enable the external party to access data of the cloud service users.
Inappropriate use of System Infrastructure: "The risk is that authorized users of a company's network may use the network for non-business uses such as inappropriate web browsing. This may result in litigation accusing employers and cloud service providers of employee harassment." (Agarwal & Agarwal, 2011, p. 258)

Session hijacking: Similar to eavesdropping, session hijacking is the risk that an external party is able to take over the connection between the client and server. This enables the external party to post as the original user, in turn giving the possibility to do everything the user is able to do.

Note. Adapted from Agarwal and Agarwal (2011). Underlined vulnerabilities are seen as (partially) preventable by users of the cloud service.

With the implementation of Big Data, a number of information security risks present themselves. This is especially the case when dealing with "sensitive information regarding customers and employees, as well as intellectual property, trade secrets and financial information" (Tankard, 2012). Additionally, having all the data centralized makes it a valuable target, making "it essential that Big Data stores are properly controlled and protected" (Tankard, 2012).

Even with the protection of Big Data being essential, businesses using Big Data "may not have the fundamental assets particularly from a security perspective" (Inukollu et al., 2014, p. 49). Furthermore, "If a security breach occurs to Big Data, it would result in even more serious legal repercussions and reputational damage than at present" (Inukollu et al., 2014, p. 49).

5.5.5 Framework

Table 11				
	Confidentiality			Referenced from
Access control	1	Establish and maintain an inventory of accounts.	“Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person’s name, username, start/stop dates, and department. Validate that all active accounts are authorized properly and inactive accounts are removed, on a recurring schedule at a minimum quarterly, or more frequently.”	CIS Security Controls – control 5.1
	2	Use unique passwords.	“Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.”	CIS Security Controls – control 5.2
	3	Centralize access control.	“Centralize access control for all enterprise assets through a directory service or SSO provider, if and where supported.”	CIS Security Controls – control 6.7
	4	Train workforce members on authentication best practices.	“Example topics include MFA, password composition, and credential management.”	CIS Security Controls – control 14.3
	5	Select a strong password.	Make users create a password not easily guessed by using user related information. (e.g., names, telephone numbers and dates of birth)	Own creation
	6	Avoid keeping a record.	Avoid users keeping a record of their passwords, unless this can be stored securely in an approved method. (e.g., password vault on phone)	Own creation

	7	Avoid sharing business and private passwords.	Avoid users using a password for both business and personal use.	Own creation
	8	Change first password.	Force users to change the first password the user is given.	Own creation
	9	Manage default accounts on enterprise assets and software.	"Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable."	CIS Security Controls – control 4.7
	10	Monitoring of access control process.	"Monitor the process of access control. Review and update the access control process annually, or when significant enterprise changes occur that could impact this measure."	CIS Security Controls – control 5.2
Encryption	11	Establish and maintain a data classification scheme.	"Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this measure."	CIS Security Controls – control 3.7
	12	Encrypt data on end-users' devices.	"Encrypt data on end-user devices containing sensitive data."	CIS Security Controls – control 3.6
	13	Encrypt data on removable media.	"Encrypt data on removable media."	CIS Security Controls – control 3.9
	14	Encrypt sensitive data in transit.	"Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH)."	CIS Security Controls – control 3.10
	15	Encrypt sensitive data at rest.	"Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this measure. Additional encryption methods may include application	CIS Security Controls – control 3.11

			layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.”	
	16	Train workforce on data handling best practices.	“Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.”	CIS Security Controls – control 14.4
	17	Train workforce members on causes of unintentional data exposure.	“Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.”	CIS Security Controls – control 14.5
	18	Ensure service provider contracts include data security requirements.	“Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, […] data encryption requirements, and data disposal commitments. [..] Review service provider contracts annually to ensure contracts are not missing security requirements.”	CIS Security Controls – control 15.4
	19	Usage of encryption algorithms.	Only use established, widely acknowledged, and well tested encryption algorithms.	Own creation
	20	Securely dispose of data.	“Securely dispose of data as outlined in the enterprise’s data management process. Ensure the disposal process and method are commensurate with the data sensitivity.”	CIS Security Controls – control 3.5

Integrity				Referenced from
Security control	21	Configure data access control lists.	"Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications."	CIS Security Controls – control 3.3
	22	Establish an Access Granting Process.	"Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user."	CIS Security Controls – control 6.1
	23	Establish an Access Revoking Process.	"Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails."	CIS Security Controls – control 6.2
	24	Define and Maintain Role-Based Access Control.	"Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently."	CIS Security Controls – control 6.8
Reliability control	25	Establish and maintain a secure configuration process for enterprise assets. Configuration Management Database (CMDB)	"Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this measure."	CIS Security Controls – control 4.1

	26	Implement and manage a firewall on servers.	“Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.”	CIS Security Controls – control 4.4
	27	Implement and manage a firewall on end-user devices.	“Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.”	CIS Security Controls – control 4.5
	28	Uninstall or disable unnecessary services on enterprise assets and software.	“Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.”	CIS Security Controls – control 4.8
Awareness control	29	Establish and maintain a security awareness program.	“Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise’s workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this measure.”	CIS Security Controls – control 14.1
Audit control	30	Establish and maintain an audit log management process.	“Establish and maintain an audit log management process that defines the enterprise’s logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this measure.”	CIS Security Controls – control 8.1
	31	Collect audit logs.	“Collect audit logs. Ensure that logging, per the enterprise’s audit log management process, has been enabled across enterprise assets.”	CIS Security Controls – control 8.2

	32	Collect detailed audit logs.	“Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.”	CIS Security Controls – control 8.5
	33	Ensure adequate audit log storage.	“Ensure that logging destinations maintain adequate storage to comply with the enterprise’s audit log management process.”	CIS Security Controls – control 8.3
Additional measures	34	Implement digital signatures.	Implement digital signatures and add these signatures to every addition, modification or other action. This will provide an origin of the action by associating the action to a user and thus preventing deniability.	Own creation
	35	Implement data fault tolerance.	Implement techniques to prevent faults in data. This can be done for example by implementing data redundancy techniques such as RAID or mirroring.	Own creation
	36	Establish and maintain an inventory of service providers.	“Establish and maintain an inventory of service providers, such as cloud, internet and application server providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this measure.”	CIS Security Controls – control 15.1
	37	Assess service providers.	“Assess service providers consistent with the enterprise’s service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.”	CIS Security Controls – control 15.5

Availability				Referenced from
Maintenance of software and hardware	38	Establish and maintain a software inventory.	"Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. This information is added to the Configuration Management Database. Review and update the software inventory bi-annually, or more frequently."	CIS Security Controls – control 2.1
	39	Ensure authorized software is currently supported.	"Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently."	CIS Security Controls – control 2.2
	40	Address unauthorized software.	"Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently."	CIS Security Controls – control 2.3
	41	Ensure network infrastructure is up-to-date.	"Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software. Review software versions monthly, or more frequently, to verify software support."	CIS Security Controls – control 12.1

	42	Train workforce on how to identify and report if their enterprise assets are missing security updates.	"Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools."	CIS Security Controls – control 14.7
Maintenance of technical infrastructure	43	Establish and maintain a secure configuration process for network infrastructure.	"Establish and maintain a secure configuration process for network devices like switches, access points and repeaters. Review and update documentation annually, or when significant enterprise changes occur that could impact this measure."	CIS Security Controls – control 4.2
Disaster recovery plan	44	Establish and Maintain a Data Recovery Process.	"Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this measure."	CIS Security Controls – control 11.1
	45	Perform automated backups.	"Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data."	CIS Security Controls – control 11.2
	46	Protect recovery data.	"Protect recovery data with equivalent controls to the original data. Ensure recovery data cannot be corrupted or locked in a cyberattack. Reference encryption or data separation, based on requirements."	CIS Security Controls – control 11.3
	47	Establish and maintain an isolated instance of recovery data.	"Establish and maintain an isolated instance of recovery data on an independent node. Example implementations include version controlling backup destinations through offline, cloud, or off-site systems or services."	CIS Security Controls – control 11.4

	48	Ensure service provider contracts include security incident requirements.	"Ensure service provider contracts include security requirements. Example requirements may include […] security incident and/or data breach notification and response. […] Review service provider contracts annually to ensure contracts are not missing security requirements."	CIS Security Controls – control 15.4
	49	Designate personnel to manage incident handling.	"Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this measure."	CIS Security Controls – control 17.1
	50	Establish and maintain contact information for reporting security incidents.	"Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date."	CIS Security Controls – control 17.2
	51	Establish and maintain an enterprise process for reporting incidents.	"Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this measure."	CIS Security Controls – control 17.3

Access removal controls	52	Configure automatic session locking on enterprise assets.	"Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes."	CIS Security Controls – control 4.3
	53	Enforce automatic device lockout on portable end-user devices.	"Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts."	CIS Security Controls – control 4.10
	54	Enforce remote wipe capability on portable end-user devices.	"Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise."	CIS Security Controls – control 4.11
Devices on the network	55	Establish and maintain detailed enterprise asset inventory.	"Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently."	CIS Security Controls – control 1.1

	56	Utilize an active discovery tool.	"Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently."	CIS Security Controls – control 1.3
	57	Address unauthorized assets.	"Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset."	CIS Security Controls – control 1.2
	58	Separate enterprise workspaces on mobile end-user devices.	"Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. This is to separate enterprise applications and data from personal applications and data."	CIS Security Controls – control 4.12
Working locations	59	Require MFA for remote network access.	"Require MFA for remote network access."	CIS Security Controls – control 6.4
Cyber resilience	60	Monitoring and response on cybersecurity.	Monitor network data traffic on cyber-attacks and create (automated) responses. Perform reviews of cybersecurity responses to validate that responses are robust enough, on a recurring schedule at a minimum quarterly, or more frequently.	Own creation
	61	Establish and maintain a penetration testing program.	"Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements."	CIS Security Controls – control 18.1

	62	Perform periodic external penetration tests.	“Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.”	CIS Security Controls – control 18.2
	63	Remediate penetration test findings.	“Remediate penetration test findings based on the enterprise’s policy for remediation scope and prioritization.”	CIS Security Controls – control 18.3

Table 12		
Internet of Things		
	Explanation	Important/relevant measures
Sensing layer	The layer which contains hardware such as sensors and actuators.	11, 14, 17, 19, 25, 27, 28, 41, 55, 56, 57, 61, 62, 63
Network layer	The layer containing physical infrastructure in support of connectivity between sensing layer and service layer.	41, 43, 60, 61, 62, 63
Service layer	This layer contains data storage and processing for the creation and management of services needed for interfacing with users or applications.	11, 13, 15, 18, 19, 20, 21, 22, 23, 24, 26, 28, 35, 44, 45, 46, 47, 48, 49, 60, 61, 62, 63
Interface layer	This layer contains the methods for interacting with users or applications, such as APIs and interfaces.	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 16, 17, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32, 33, 34, 38, 39, 40, 41, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63
Cloud solutions		
	Explanation	Important/relevant measures
Applications	Application that runs on the server.	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 16, 17, 18, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 40, 41, 42, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63
Data	Databases.	11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 44, 45, 46, 47, 48, 49, 50, 51, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63

Runtime	Keeping all processes running.	36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 61, 62, 63
Middleware	Software acting as a bridge between an operating system and databases or applications.	11, 14, 25, 28, 30, 31, 32, 33, 36, 37, 38, 39, 40, 41, 42, 49, 50, 51, 60, 61, 62, 63
Operating system	Operating system.	25, 29, 31, 36, 37, 38, 39, 40, 41, 42, 49, 50, 51, 60, 61, 62, 63
Visualization	Creation of virtual servers, infrastructures, devices and computing resources.	27, 29, 36, 37, 49, 50, 51, 61, 62, 63
Servers	A computer program or device that provides a service to another computer program and its user.	26, 36, 37, 43, 49, 50, 51, 55, 60, 61, 62, 63
Storage	Storage of data.	11, 13, 14, 15, 18, 19, 20, 21, 22, 23, 24, 35, 36, 37, 44, 45, 46, 47, 48, 49, 60, 61, 62, 63
Networking	Linking of computers to allow them to operate interactively.	37, 41, 43, 54, 60, 61, 62, 63
Big Data		
	Explanation	Important/relevant measures
Network level	Related to network protocols and security, like distributed nodes and data.	26, 41, 43, 60, 61, 62, 63
Authentication level	Related to encryption and decryption techniques, logging and general authentication methods.	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 18, 19, 21, 22, 23, 24, 30, 31, 32, 33, 52, 53, 54, 59, 61, 62, 63
Data level	Relates to general integrity and availability challenges.	28, 29, 34, 35, 36, 37, 42, 44, 45, 46, 47, 48, 49, 60, 61, 62, 63
Generic types	Relates to traditional security tools and security related to the use of other technologies.	25, 26, 27, 38, 39, 40, 50, 51, 55, 56, 57, 58, 60, 61, 62, 63

Table 13			
Cloud solutions			
On-site	IaaS	PaaS	SaaS
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Operating system	Operating system	Operating system	Operating system
Visualization	Visualization	Visualization	Visualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking
Legend:	Customer manages	Cloud service provider manages	

5.6 Framework Validation

Based on the feedback which was received from the interviewed expert senior colleagues, the following adjustments were made to the first version of the framework:

1. Chapter 5.1 was added;
2. Chapter 5.5.3 was added;
3. Chapter 5.5.4 was added;
4. Measure number 10 concerning monitoring of access control process was added and other numbers were adjusted accordingly;
5. Measure number 11 concerning data classification was added and other numbers were adjusted accordingly;
6. Measure number 60 concerning monitoring and response on cybersecurity was added;
7. Measure number 61 concerning establishment and maintenance of a penetration testing program was added;
8. Measure number 62 concerning the performance of periodic external penetration tests was added;
9. Measure number 63 concerning the remediation of penetration test findings was added;
10. Table 11 was split in three parts, each part beginning with an element of the CIA Triad;
11. Some clarification was added to a number of measures;
12. An Excel file was created for a more practical overview of the measures corresponding to the different technologies and their levels. This file is not directly included in this thesis;
13. Included references to original frameworks.

The customers of Baker Tilly who were also interviewed were not asked for feedback. This is due to the knowledge and experience gap, which was estimated to be too large for appropriate feedback. The creation and validation of a framework was estimated not to be within their expertise. Senior colleagues were found to be able to provide feedback based on their knowledge and experience.

6. Discussion

This chapter serves as a reflection of the research process and the outcome of the research. This will be done by firstly stating and discussing the limitations which could influence the usability of the research. Following this, design research guidelines by Hevner et al. (2004) will be used to assess this research. Finally, the research's academic and practical implications are discussed.

6.1 Limitations

This research has several limitations. The first limitation is the lack of respondents for primary data. During the process of contacting the respondents, six businesses and three experts were contacted. After multiple reminders, out of the six businesses, only four responded, and of these four, only two agreed to an interview. All three experts did agree to an interview. This might have resulted in the primary data being skewed more towards the types of businesses, experiences and requirements of those which were interviewed, instead of a more general overview of manufacturing SMEs. This can lead to the framework being more applicable to metalworking SMEs instead of general manufacturing SMEs, as the two interviewed businesses are both in the metalworking industry.

The second limitation is the lack of time available to create an information security framework from the ground up, resulting in an even more specialized framework. As such a project could take years, this was not realistic in the timeframe set for this thesis. Instead of creating the framework from the ground up, it was chosen that the framework would be created through information security best practices from a number of existing frameworks and requirements from both primary and secondary data.

The third limitation is the lack of real-world validation of the framework. This was not done as the implementation of an information security framework could, depending on the complexity of the business and its environment, take many months or even years. As such a timeframe was not in the scope of this thesis, this type of validation was not executed. However, validation through expert senior colleagues was executed. The customers of Baker Tilly who were also interviewed were not asked for feedback. This is due to the knowledge and experience gap, which was estimated to be too large for appropriate feedback. The creation and validation of a framework was estimated not to be within their expertise.

The final limitation is the lack of possibility for non-verbal communication during the interviews. As all of the interviews were conducted via Microsoft Teams, communication was limited to what could be seen and heard through the webcam.

6.2 Design Research Guidelines

The effectiveness of this research is examined with the use of the design science research guidelines as developed by Hevner et al. (2004), which is displayed in Table 14.

Table 14

Design-science research guidelines.

Guideline	Description
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Note. Referenced from Hevner et al. (2004)

6.2.1 Design as an Artifact

In this research, an artifact in the shape of a framework was developed. This framework is designed to help manufacturing SMEs implement a secure baseline of information security measures during and after the implementation of certain Industry 4.0 technologies. The selected technologies are Internet of Things, cloud solutions and Big Data.

6.2.2 Problem Relevance

Industry 4.0 technologies are being implemented more and more often. As these technologies create, transfer and store a large amount of data, the importance for proper information security also grows.

This results in the requirement for a specialized information security framework becoming quite relevant, as this is currently not available.

6.2.3 Design Evaluation

The framework has mainly been evaluated by three expert senior colleagues at Baker Tilly. Following these evaluations, a number of adjustments were made on the initial version of the framework. After these adjustments, it was concluded that the framework was complete, usable and useful. As indicated in the limitations, no real-world validation could be completed, due to time constraints.

6.2.4 Research Contributions

As mentioned in the implications, this research is the first to create a baseline information security framework specifically for the implementation of Internet of Things, cloud solutions and/or Big Data in manufacturing SMEs.

6.2.5 Research Rigor

This research leans on the foundations of literature about the CIA Triad, Internet of Things, cloud solutions and Big data, as well as interviews and information security frameworks. To process this information and construct the framework, a number of different methodologies were used. For the literature, no specific pre-existing method was used. For the qualitative data, semi-structured interviews, combined with axial coding during processing, were used. Finally, for the evaluation of the framework, knowledge of experts was used, based on a predetermined set of questions and discussion points. The methodologies are more extensively explained in chapter 3.

6.2.6 Design as a Search Process

During the research, multiple alterations were made to the scope of the framework and the framework itself. Each alteration improved the quality of the framework. Internet of Things, cloud solutions and Big Data were chosen as the technologies due to the relevance as found in the literature. A technology which was removed early on in the research, due to lack of relatedness with the other technologies, was Artificial Intelligence. Based on the literature and list of customers at Baker Tilly, a similar choice was made to focus on manufacturing SMEs, instead of all types of SMEs.

6.2.7 Communication of Research

The framework is designed to be usable by anyone with some knowledge about IT. This requirement results in the framework being able to be easily presented to technology-oriented audiences. For management-oriented audiences, most elements should be comprehensible.

6.2.8 Conclusion

According to Hevner et al. (2004), “the fundamental principle of design-science research from which our seven guidelines are derived is that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artifact.” Additionally, Hevner et al. (2004) state that the purpose for the guidelines is “to assist researchers, reviewers, editors, and readers to understand the requirements for effective design-science research.” Following the guidelines and how these are reflected in the thesis, it can be argued that the design-science research has been effective and knowledge and understanding of the problem and its solution are acquired.

6.3 Implications

The results of this thesis have a number of implications for future research and practical use. These implications are split into the appropriate group in this chapter.

6.3.1 Academic Implications

This research and the framework developed during the research has implications for future research. This research is the first to create a framework of baseline information security measures for a manufacturing SMEs wanting to implement Internet of Things, cloud solutions and/or Big Data. This gives other studies a starting point for future research on this topic. Additionally, it gives other studies a starting topic for new research on a similar topic.

6.3.2 Practical Implications

The framework created aids manufacturing SMEs with the implementation of a proper baseline of information security when implementing Internet of Things, cloud solutions and/or Big Data. As several participants stated that such a framework did not exist previously, this framework fills that hole.

Additionally, this research can prove to businesses that information security is not only something that costs a lot of money and is complicated, but that information security is very useful and can save a lot of money when it prevents issues of any kind.

Finally, the framework can help businesses who have implemented some information security measures to get an overview whether there are any points which are not implemented yet, or are not implemented correctly.

Overall, this research can help businesses improve their information security without needing any external advisors to successfully implement the framework.

7. Conclusion

This chapter will serve as the conclusion of this research. It will start by answering the sub-questions stated in chapter 1.3 to help answer the central research question. Following this, recommendations are given for future research.

7.1 Research Questions

The following is a description of the research's central research question:

“How can information be kept secure with a risk-based approach when implementing Industry 4.0 technologies in the SME manufacturing industry?”

To answer this, an extensive literature study and 5 interviews were conducted. The research results and resulting framework were validated by three experts who are active in the field of information security and manufacturing SMEs. The following three sub-questions were formulated to help answer the central research question. These sub-questions will be discussed below.

1. *What are the components and what is the value of the chosen Industry 4.0 technologies?*

To answer the first sub-question, the literature study was used as a foundation. The value of an Internet of Things (IoT) infrastructure was found to lie within the ability to facilitate the connection between interrelated computing devices or other ‘things’ over a network without any form of human interaction. This is achieved by implementing an infrastructure consisting of multiple layers. These are the sensing, network, service and interface layers.

Cloud solutions are internet-based IT resources which can be requested on demand from cloud service providers. These cloud solutions are able to scale up or down quickly and on demand in order to meet business needs. This ability to meet demand is why using cloud solutions alongside an IoT implementation can be very valuable to the cloud user due to the flexibility of the cloud service and its cost. Without an IoT implementation, the ability to meet demand can still be as valuable for businesses.

Big Data refers to a dataset which is not able to be processed by traditional tools or methods due to the immense volume, velocity and variety. This data can be used to gain new insights and knowledge of customers or processes. Therefore, when an organization decides to, for example, implement an IoT application, which creates a lot of data, implementing Big Data is a logical step to take.

Finally, the value of the three technologies combined was found to lie within the synergy that can come from the implementation of a combination of the technologies.

2. How do these components influence data security in a SME?

For all three technologies, information security is imperiled in the network-based system because of the threats appearing during and after implementation. Each technology brings its own additions and modifications to the business, which can open the door to new ways for information security breaches to occur.

For IoT, availability of the data is important in each of the layers. The reason is that if one of the layers becomes unavailable for any reason, the entire system may stop being available. Additionally, issues related to encryption of data, internet connectivity, software protection, and authorization make the IoT system vulnerable to external security risks. It can be concluded that the Internet of Things has an impact on the security and privacy of the involved stakeholders.

To keep this impact at a minimum, private enterprises using an IoT technology will have to include resilience to attacks, data authentication, access control, and client privacy into their risk management concept, among other measures.

With the use of cloud services, a different focus on information security needs to be made. Compared to having everything on-site, using cloud services makes the service provider responsible for most information security, depending on the type of cloud service used. However, certain things, such as internal password security and incorrect data entries causing integrity failures, will stay the responsibility of the business.

A service level agreement is to be used to note the responsibility and accountability of the cloud service provider, whilst also giving the business an overview of which measures are not taken care of.

With the implementation of Big Data, a number of information security issues are found to present themselves, especially when having all the data centralized. This is due to the large volume of data, causing a breach to result in serious legal repercussions and reputational damage compared to smaller datasets. The issues and challenges with Big Data can be split into four levels: the network level, the authentication level, the data level and generic types. With each level concerning a different part of information security and needing different measures.

3. Which measures lay the basis for solid information security?

From the analysis of the existing frameworks, it is concluded that these frameworks are a collection of generic measures which do not provide a baseline or relevant measures in certain scenarios. This is especially the case when wanting to implement a specific technology.

To create a baseline of information security measures, the CIA Triad was partitioned, analyzed and cross-examined with the existing frameworks for relevant information security measures. This analysis provided 63 measures, which were consequently assigned to the relevant parts of the technologies. This overview can be seen in tables 11 and 12.

7.2 Recommendations

This section provides recommendations for organizations and recommendations for future research. The recommendations were discovered in the course of this study and are discussed below.

7.2.1 Recommendations for Organizations

The possibly most important takeaway for businesses is to implement proper information security as soon as possible. Update this information security over time and when implementing new technologies or machines. Do not wait until breaches happen to businesses close by, but keep ahead of the threats. This may require a switch of mindset to not see information security as cost without benefit, but to see it as a necessary investment to protect the information of the business and its stakeholders.

Additionally, prevent having to play catch-up on information security whilst the technology is already implemented, as this could result in threats finding the weaknesses quicker than the business.

7.2.2 Future Research

This research has focused on developing the first framework for the implementation of an information security baseline for manufacturing SMEs wanting to implement IoT, cloud solutions and/or Big Data. Although it is unknown whether a similar artifact for a different type of business and/or technology has been created before, it is an idea which other studies could repeat. Additionally, this research can be extended upon by creating the framework from the ground up, instead of relying on the best practices of existing information security frameworks.

Furthermore, this research can be continued by validating the framework in multiple real-world scenarios. This would make for better validation and can prove that the framework is indeed fully functional and ready for businesses to use.

Finally, a government mandated standard for information security within Industry 4.0, or a subset of these technologies, could prove to be of use to many SMEs. Currently, the standards are not designed for every type of business and do not include all technologies within Industry 4.0, resulting in incomplete information security.

8. Bibliography

27001 Academy. (n.d.). *What is ISO 27001? A beginner's guide.* Retrieved March 24, 2022, from https://advisera.com/27001academy/what-is-iso-27001/

Agarwal, A., & Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. *International Journal of Computer Applications in Engineering Sciences*, *1*, 257–259. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.207.9119&rep=rep1&type=pdf

Ahmed, E., Yaqoob, I., Hashem, I. A. T., Khan, I., Ahmed, A. I. A., Imran, M., & Vasilakos, A. V. (2017). The role of big data analytics in Internet of Things. *Computer Networks*, *129*, 459–471. https://doi.org/10.1016/j.comnet.2017.06.013

All Answers Ltd. (2021, December 31). *Aadhar Breach – A Case of Data Privacy in India*. UKEssays. Retrieved March 23, 2022, from https://www.ukessays.com/essays/information-technology/aadhar-breach-a-case-of-data-privacy-in-india.php

Aloul, F., Zahidi, S., & El-Hajj, W. (2009, May). Two factor authentication using mobile phones. *2009 IEEE/ACS International Conference on Computer Systems and Applications*, 641–644. https://doi.org/10.1109/aiccsa.2009.5069395

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). Internet of Things: Security vulnerabilities and challenges. *2015 IEEE Symposium on Computers and Communication (ISCC)*. https://doi.org/10.1109/iscc.2015.7405513

Awati, R. (2021, August 20). *nonrepudiation*. SearchSecurity. Retrieved March 31, 2022, from https://www.techtarget.com/searchsecurity/definition/nonrepudiation

Awwad, K. A., Shibani, A., & Ghostin, M. (2020). Exploring the critical success factors influencing BIM level 2 implementation in the UK construction industry: the case of SMEs. *International Journal of Construction Management*, 1–8. https://doi.org/10.1080/15623599.2020.1744213

Bell, D. E., LaPadula, L. J., & MITRE CORP BEDFORD MA. (1973). *Secure computer systems: Mathematical foundations* (No. AD0770768). National Technical Information Service. https://apps.dtic.mil/sti/pdfs/AD0770768.pdf

Bernard, P. (2012). *COBIT® 5 - A Management Guide*. Van Haren Publishing.

Blili, S., & Raymond, L. (1993). Information technology: Threats and opportunities for small and medium-sized enterprises. *International Journal of Information Management*, *13*(6), 439–448. https://doi.org/10.1016/0268-4012(93)90060-h

Bowell, I. (2021, December 8). *New in Information Security: A Look at ISO 27001 and 27002*. Edge Technology Group. Retrieved May 5, 2022, from https://www.edgetg.com/information-security-iso-27001-27002/

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004). Economics of IT Security Management: Four Improvements to Current Security Practices. *Communications of the Association for Information Systems*, *14*(1), 65–75. https://doi.org/10.17705/1cais.01403

Center for Internet Security. (2022, February 4). *CIS Controls Version 8*. CISecurity. Retrieved April 14, 2022, from https://www.cisecurity.org/controls/v8

Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer*, *44*(4), 91–93. https://doi.org/10.1109/mc.2011.115

Clark, D. D., & Wilson, D. R. (1987, April). A Comparison of Commercial and Military Computer Security Policies. *1987 IEEE Symposium on Security and Privacy*, 184–194. https://doi.org/10.1109/sp.1987.10001

Culot, G., Nassimbeni, G., Orzes, G., & Sartor, M. (2020). Behind the definition of Industry 4.0: Analysis and open questions. *International Journal of Production Economics*, *226*. https://doi.org/10.1016/j.ijpe.2020.107617

Daniel, B. (2021, May 4). *Symmetric vs. Asymmetric Encryption: What's the Difference?* Trenton Systems. Retrieved March 31, 2022, from https://www.trentonsystems.com/blog/symmetric-vs-asymmetric-encryption

Datashield. (n.d.). *SCADA & IoT Definition | Cybersecurity risks explained*. Datashieldprotect. Retrieved April 14, 2022, from https://www.datashieldprotect.com/blog/what-is-scada-iot#:%7E:text=IoT%20systems%20include%20interrelated%20devices,and%20functionality%20where%20SCADA%20ends.

De Ondernemer. (2020, November 25). *Je bedrijf is veilig voor een cyberaanval? Die gedachte maakt je juist kwetsbaar*. De Onderneming. Retrieved March 23, 2022, from https://www.deondernemer.nl/innovatie/cybersecurity/bedrijf-veilig-cyberaanval-kwetsbaar~2556543

del Vecchio, L. (2021, December 13). *What Is A Cloud Based Solution? Definition and Meaning*. PLANERGY Software. Retrieved April 18, 2022, from https://planergy.com/blog/cloud-based-solutions/

Deloitte Insights. (2020). *The Fourth Industrial Revolution.* https://www2.deloitte.com/content/dam/Deloitte/de/Documents/human-capital/Deloitte_Review_26_Fourth_Industrial_Revolution.pdf

Delve. (2022, February 8). *How To Do Open, Axial, & Selective Coding in Grounded Theory*. Retrieved May 2, 2022, from https://delvetool.com/blog/openaxialselective

Erboz, G. (2017). How to Define Industry 4.0: The Main Pillars Of Industry 4.0. *Managerial trends in the development of enterprises in globalization era*, 761–767.

ERM Protect. (2019, July 11). *ISO 27000: Plan - Do - Check - Act*. Retrieved April 13, 2022, from https://ermprotect.com/blog/iso-27000-plan-do-check-act/

European Commission. (n.d.). *SME definition*. Internal Market, Industry, Entrepreneurship and SMEs. Retrieved February 10, 2022, from https://ec.europa.eu/growth/smes/sme-definition_en

Florêncio, D., & Herley, C. (2007, May). *A Large-Scale Study of Web Password Habits*. International World Wide Web Conference, Banff, Alberta, Canada.

Grefen, P. W., & Apers, P. M. (1993). Integrity control in relational database systems — an overview. *Data & Knowledge Engineering*, *10*(2), 187–223. https://doi.org/10.1016/0169-023x(93)90008-d

Herley, C. (2009). So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. *NSPW*.

Hern, A. (2017, February 21). *Did your Adobe password leak? Now you and 150m others can check*. The Guardian. Retrieved March 23, 2022, from https://www.theguardian.com/technology/2013/nov/07/adobe-password-leak-can-check

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Horváth, D., & Szabó, R. Z. (2019). Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities? *Technological Forecasting and Social Change*, *146*, 119–132. https://doi.org/10.1016/j.techfore.2019.05.021

Humblot, N. (2021, December 2). *IoT and Big Data: Understanding the relationship between these two technologies*. Ryax Technologies. Retrieved April 19, 2022, from https://ryax.tech/iot-and-big-data-understanding-the-relationship-between-these-two-technologies/#:%7E:text=IoT%20and%20Big%20Data%20are,and%20processing%20of%20this%20data.

Inukollu, V. N., Arsi, S., & Rao Ravuri, S. (2014). Security Issues Associated with Big Data in Cloud Computing. *International Journal of Network Security & Its Applications*, *6*(3), 45–56. https://doi.org/10.5121/ijnsa.2014.6304

ISACA. (2019, April 11). *COBIT 2019 and Risk Management* [Framework Presentation]. ISACA Risk Event, Amsterdam, Netherlands.

ISO/IEC. (2013a). *ISO/IEC 27001:2013*. ISO/IEC.

ISO/IEC. (2013b). *ISO/IEC 27002:2013*. ISO/IEC.

Joy, A. (2021, August 10). *What is Cloud Computing? Definition, Examples, & Uses*. Network Coverage. Retrieved April 18, 2022, from https://www.netcov.com/what-is-cloud-computing/

Kamble, S. S., Gunasekaran, A., Parekh, H., & Joshi, S. (2019). Modeling the internet of things adoption barriers in food retail supply chains. *Journal of Retailing and Consumer Services*, *48*, 154–168. https://doi.org/10.1016/j.jretconser.2019.02.020

Kandukuri, B. R., V., R. P., & Rakshit, A. (2009). *Cloud Security Issues*. 517–520. https://doi.org/10.1109/scc.2009.84

Kerckhoffs, A. (1883). La cryptographic militaire. *Journal Des Sciences Militaires*, *IX*, 5–83.

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. *Procedia Computer Science*, *125*, 691–697. https://doi.org/10.1016/j.procs.2017.12.089

Kushner, D. (2013). The real story of stuxnet. *IEEE Spectrum*, *50*(3), 48–53. https://doi.org/10.1109/mspec.2013.6471059

Layton, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications*, *19*(6), 321–330. https://doi.org/10.1016/j.jisa.2014.10.012

Lee, J., Bagheri, B., & Kao, H. A. (2015). A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, *3*, 18–23. https://doi.org/10.1016/j.mfglet.2014.12.001

Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Lin, C. L., & Fan, K. C. (2004). Biometric Verification Using Thermal Images of Palm-Dorsa Vein Patterns. *IEEE Transactions on Circuits and Systems for Video Technology*, *14*(2), 199–213. https://doi.org/10.1109/tcsvt.2003.821975

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, *03*(05), 164–173. https://doi.org/10.4236/jcc.2015.35021

Masood, T., & Sonntag, P. (2020). Industry 4.0: Adoption challenges and benefits for SMEs. *Computers in Industry*, *121*, 103261. https://doi.org/10.1016/j.compind.2020.103261

Metzger, P. (2021, December 1). *What is a SCADA System and How Does It Work?* Onlogic. Retrieved April 14, 2022, from https://www.onlogic.com/company/io-hub/what-is-a-scada-system-and-how-does-it-work/

Moen, R., & Norman, C. (2006). *Evolution of the PDCA Cycle*.

Monterie, A. (2021, November 9). *VDL overleefde cyberaanval dankzij backups*. Computable.nl. Retrieved March 22, 2022, from https://www.computable.nl/artikel/nieuws/security/7270830/250449/vdl-overleefde-cyberaanval-dankzij-backups.html

Nauman, A., Qadri, Y. A., Amjad, M., Zikria, Y. B., Afzal, M. K., & Kim, S. W. (2020). Multimedia Internet of Things: A Comprehensive Survey. *IEEE Access*, *8*, 8202–8250. https://doi.org/10.1109/access.2020.2964280

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Oracle. (n.d.). *Wat is big data? | Oracle Nederland*. Retrieved April 19, 2022, from https://www.oracle.com/nl/big-data/what-is-big-data/

Orzes, G., Rauch, E., Bednar, S., & Poklemba, R. (2018). Industry 4.0 Implementation Barriers in Small and Medium Sized Enterprises: A Focus Group Study. *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 1348–1352. https://doi.org/10.1109/ieem.2018.8607477

PCI Security Standards Council. (2022, March 1). *Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards*. Retrieved May 5, 2022, from https://www.pcisecuritystandards.org/

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). *A Design Science Research Methodology for Information Systems Research* (Vol. 24, Issue 3). Informa UK Limited. https://doi.org/10.2753/mis0742-1222240302

Professor Wolfgang Wahlster. (n.d.). Deutsches Forschungszentrum Für Künstliche Intelligenz. Retrieved March 31, 2022, from http://www.dfki.de/%7Ewahlster/

Qadir, S., & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, *07*(03), 185–194. https://doi.org/10.4236/jis.2016.73014

Ranganathan, K., Iamnitchi, A., & Foster, I. (2002, May). Improving Data Availability through Dynamic Model-Driven Replication in Large Peer-to-Peer Communities. *2nd IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID'02)*. https://doi.org/10.1109/ccgrid.2002.1017164

Red Hat. (2018, March 15). *Types of cloud computing*. Retrieved April 18, 2022, from https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud

Rojko, A. (2017). Industry 4.0 Concept: Background and Overview. *International Journal of Interactive Mobile Technologies (iJIM)*, *11*(5), 77. https://doi.org/10.3991/ijim.v11i5.7072

Roncevich, T. (2018, March 7). *What is the ISO 27001 and Do You Need It?* Cyberguard Compliance. Retrieved April 13, 2022, from https://info.cgcompliance.com/blog/what-is-the-iso-27001-and-do-you-need-it

Safar, L., Sopko, J., Bednar, S., & Poklemba, R. (2018). Concept of SME business model for industry 4.0 environment. *TEM Journal*, *7*(3), 626–637. https://doi.org/10.18421/TEM73-20

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

SAS. (n.d.). *Big Data: What it is and why it matters*. Retrieved April 19, 2022, from https://www.sas.com/nl_nl/insights/big-data/what-is-big-data.html

Shewhart, W. A. (1939). *Statistical method from the viewpoint of quality control*. The Graduate School, The Deparment of Agriculture.

Sivathanu, G., Wright, C. P., & Zadok, E. (2005). Ensuring data integrity in storage. *Proceedings of the 2005 ACM Workshop on Storage Security and Survivability - StorageSS '05*, 26–36. https://doi.org/10.1145/1103780.1103784

Steve, S. (2020, August 27). *Facts About the Adobe Data Breach*. Cygilant. Retrieved March 23, 2022, from https://blog.cygilant.com/blog/bid/326184/facts-about-the-adobe-data-breach

Suse. (n.d.). *What are Cloud Solutions? | Answer from*. SUSE Defines. Retrieved April 18, 2022, from https://www.suse.com/suse-defines/definition/cloud-solutions/

Szajna, A., Stryjski, R., Woźniak, W., Chamier-Gliszczyński, N., & Kostrzewski, M. (2020). Assessment of Augmented Reality in Manual Wiring Production Process with Use of Mobile AR Glasses. *Sensors*, *20*(17), 4755. https://doi.org/10.3390/s20174755

Tankard, C. (2012). Big data security. *Network Security*, *2012*(7), 5–8. https://doi.org/10.1016/s1353-4858(12)70063-6

VNG. (2021, April 29). *Handreiking Information Security Management System (ISMS) BIO en AVG*. Informatiebeveiligingsdienst. Retrieved May 20, 2022, from https://www.informatiebeveiligingsdienst.nl/product/isms-v1-0/

vom Brocke, J., Hevner, A., & Maedche, A. (2020). *Design Science Research. Cases*. Springer Publishing. https://doi.org/10.1007/978-3-030-46781-4

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

Weber, R. H., & Weber, R. (2010). *Internet of Things*. Springer Publishing. https://doi.org/10.1007/978-3-642-11710-7

Weiß, P., Kölmel, B., & Bulander, R. (2016, September). Digital Service Innovation and Smart Technologies: Developing Digital Strategies based on Industry 4.0 and Product Service Systems for the Renewal Energy Sector. In T. Russo-Spena & C. Mele (Eds.), *What's ahead in service research* (pp. 274–291). RESER.

Wieringa, R. J. (2014). *Design Science Methodology for Information Systems and Software Engineering*. Springer Publishing. https://doi.org/10.1007/978-3-662-43839-8

Williams, M., & Moser, T. (2019). The art of coding and thematic exploration in qualitative research. *International Management Review*, *15*(1), 45–55.

Wortmann, F., & Flüchter, K. (2015). Internet of Things. *Business & Information Systems Engineering*, *57*(3), 221–224. https://doi.org/10.1007/s12599-015-0383-3

9. Appendix

Table A1

14 Domains listed in ISO/IEC 27001 and ISO/IEC 27002.

A.5. Information security policies: The controls in this section describe how to handle information security policies.
A.6. Organization of information security: The controls in this section provide the basic framework for the implementation and operation of information security by defining its internal organization (e.g., roles, responsibilities, etc.), and through the organizational aspects of information security, like project management, use of mobile devices, and teleworking.
A.7. Human resource security: The controls in this section ensure that people who are under the organization's control are hired, trained, and managed in a secure way; also, the principles of disciplinary action and terminating the agreements are addressed.
A.8. Asset management: The controls in this section ensure that information security assets (e.g., information, processing devices, storage devices, etc.) are identified, that responsibilities for their security are designated, and that people know how to handle them according to predefined classification levels.
A.9. Access control: The controls in this section limit access to information and information assets according to real business needs. The controls are for both physical and logical access.
A.10. Cryptography: The controls in this section provide the basis for proper use of encryption solutions to protect the confidentiality, authenticity, and/or integrity of information.
A.11. Physical and environmental security: The controls in this section prevent unauthorized access to physical areas, and protect equipment and facilities from being compromised by human or natural intervention.
A.12. Operations security: The controls in this section ensure that the IT systems, including operating systems and software, are secure and protected against data loss. Additionally, controls in this section require the means to record events and generate evidence, periodic verification of vulnerabilities, and make precautions to prevent audit activities from affecting operations.
A.13. Communications security: The controls in this section protect the network infrastructure and services, as well as the information that travels through them.
A.14. System acquisition, development and maintenance: The controls in this section ensure that information security is taken into account when purchasing new information systems or upgrading the existing ones.

A.15. Supplier relationships: The controls in this section ensure that outsourced activities performed by suppliers and partners also use appropriate information security controls, and they describe how to monitor third-party security performance.
A.16. Information security incident management: The controls in this section provide a framework to ensure the proper communication and handling of security events and incidents, so that they can be resolved in a timely manner; they also define how to preserve evidence, as well as how to learn from incidents to prevent their recurrence.
A.17. Information security aspects of business continuity management: The controls in this section ensure the continuity of information security management during disruptions, and the availability of information systems.
A.18. Compliance: The controls in this section provide a framework to prevent legal, statutory, regulatory, and contractual breaches, and audit whether information security is implemented and is effective according to the defined policies, procedures, and requirements of the ISO 27001 standard.

Note: 14 domains of ISO/ IEC 27001 and ISO/IEC 27002 (ISO/IEC, 2013a; *What Is ISO 27001? A Beginner's Guide.*, n.d.).

Table A2

Categories addressed in the NIST Cyber Security Framework.

Function / Core area	**Category**
Identify	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
	Supple Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
Protect	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Detect	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.

	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
Respond	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
Recover	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

Table A2: Categories addressed in the NIST Cyber Security Framework (NIST, 2018).

Table A3

NIST 800-53 Controls.

Access Control: These controls are focused around ensuring that only authorized users are able to access critical systems and information.
Awareness and Training: The Security Awareness and Training family of controls mandate that end-users (employees) are trained in how to properly prevent, detect, and respond to cybersecurity incidents.

Audit and Accountability: These controls are designed to provide records for auditors to understand and hold users and administrators accountable for maintaining cybersecurity.
Configuration Management: Configuration management involves configuring information systems to have optimal security. Controls include change control and security impact assessments among others.
Contingency Planning: This family involves planning for incidents and contingencies to allow for optimal response.
Identification and Authentication: The Identification and Authentication family is designed to ensure that users are correctly authenticated when using networks or accessing sensitive data. Controls include the types of authentication to be used, encryption, and policies and procedures regarding authentication.
Incident Response: The Incident Response family focuses on ensuring processes are in place for quickly responding to and remediating incidents. Controls include incident response training, incident handling, monitoring for incidents, and incident handling among others.
Maintenance: This family is focused on ensuring that systems are adequately maintained. Controls include timely maintenance, controlled maintenance, and nonlocal maintenance.
Media Protection: The Media Protection family involves controls that are designed to protect media including stored media, media access, and media sanitization.
Physical and Environmental Security: Physical and Environmental Security is just as it sounds. This family of controls is less to do with cybersecurity and includes items such as disaster recovery planning, emergency power, emergency lighting, and Fire Protection.
Planning: Planning is critical for cybersecurity. Planning in NIST 800-53 involves controls around creating a system security plan, rules of behavior, and information security architecture.
Personnel Security: This family deals with security issues arising from personnel present at the facility and includes controls such as screening, termination, and policies and procedures around personnel.
Risk Assessment: This set of controls designates how a Risk Assessment should be performed, policies for performing the risk assessment, and vulnerability scanning.
Systems and Services Acquisition: These controls deal with System Development Life Cycle, Acquisition Process, and Information System Documentation among others.
Systems and Communications Protection: These controls are designed to mitigate risks from common cyberattacks such as distributed denial of service and malware. They include encryption, segmentation, VoIP security, and others.

Systems and Information Integrity: These controls are focused on ensuring the integrity of organizational information systems. Controls include error handling, spam protection, memory protection, and fail-safe procedures among others.

Table A4

CIS Security Controls.

1. Inventory and Control of Enterprise Assets: Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.
2. Inventory and Control of Software Assets: Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
3. Data Protection: Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.
4. Secure Configuration of Enterprise Assets and Software: Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
5. Account Management: Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.
6. Access Control Management: Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.
7. Continuous Vulnerability Management: Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.
8. Audit Log Management: Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

9. Email and Web Browser Protections: Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.
10. Malware Defenses: Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.
11. Data Recovery: Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.
12. Network Infrastructure Management: Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.
13. Network Monitoring and Defense: Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.
14. Security Awareness and Skills Training: Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.
15. Service Provider Management: Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.
16. Application Software Security: Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.
17. Incident Response Management: Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.
18. Penetration Testing: Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Table A5

Payment Card Industry Data Security Standard Requirements.

Goals	Requirements

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

Table A6

Solutions for Big Data challenges in the cloud.

File encryption: Since the data is present in the machines in a cluster, a hacker can steal all the critical information. Therefore, all the data stored should be encrypted. Different encryption keys should be used on different machines and the key information should be stored centrally behind strong firewalls. This way, even if a hacker is able to get the data, he cannot extract meaningful information from it and misuse it. User data will be stored securely in an encrypted manner.	Network encryption: All the network communication should be encrypted as per industry standards. The RPC procedure calls which take place should happen over SSL so that even if a hacker can tap into network communication packets, he cannot extract useful information or manipulate packets.
Logging: All the map reduce jobs which modify the data should be logged. Also, the information of users, which are responsible for those jobs should be logged. These logs should be audited	Software format and node maintenance: Nodes which run the software should be formatted regularly to eliminate any virus present. All the application software and Hadoop software

regularly to find if any, malicious operations are performed or any malicious user is manipulating the data in the nodes.	should be updated to make the system more secure.
Nodes authentication: Whenever a node joins a cluster, it should be authenticated. In case of a malicious node, it should not be allowed to join the cluster. Authentication techniques like Kerberos can be used to validate the authorized nodes from malicious ones.	Rigorous system testing of map reduce jobs: After a developer writes a map reduce job, it should be thoroughly tested in a distributed environment instead of a single machine to ensure the robustness and stability of the job.
Honeypot nodes: Honey pot nodes should be present in the cluster, which appear like a regular node but is a trap. These honeypots trap the hackers and necessary actions would be taken to eliminate hackers.	Layered framework for assuring cloud: A layered framework for assuring cloud computing consists of the secure virtual machine layer, secure cloud storage layer, secure cloud data layer, and the secure virtual network monitor layer. Cross cutting services are rendered by the policy layer, the cloud monitoring layer, the reliability layer and the risk analysis layer.
Third party secure data publication to cloud: Cloud computing helps in storing of data at a remote site in order to maximize resource utilization. Therefore, it is very important for this data to be protected and access should be given only to authorized individuals. Hence this fundamentally amounts to secure third-party publication of data that is required for data outsourcing, as well as for external publications. In the cloud environment, the machine serves the role of a third-party publisher, which stores the sensitive data in the cloud. This data needs to be protected, and the above discussed techniques have to be applied to ensure the maintenance of authenticity and completeness.	Access control: Integration of mandatory access control and differential privacy in distributed environment will be a good security measure. Data providers will control the security policy of their sensitive data. They will also control the mathematical bound on privacy violation that could take place. In the above approach, users can perform data computation without any leakage of data.

Note. Adapted from Inukollu et al. (2014).

Table A7

Prepared questions for semi-structured interview with manufacturing SME customers of Baker Tilly.

1. Could you give a short description of the company and your role(s) within the company?
2. Are you familiar with the phenomenon of 'Industry 4.0'?
3. Do you have and experience with the implementation of any technologies within the scope of Industry 4.0?
4. Have you used an information security framework for this?
5. How was the experience of using this framework?
6. Did you encounter any elements in this framework which you did not find useful or relevant?
7. Does the company employ people that are solely focused on IT or information security?

Cloud solutions

8. How is the current data storage solution organized? Are the servers on- or off-site?
9. In which way is the access control organized? Do you employ any norms for the renewal of passwords?

Internet of Things

10. In which way is the automatic production organized? Is everything fully automated, from the customer's choice to packaged order, or is everything manual?
11. Does your production system work with a SCADA system?
12. How does the company deal with incoming data? Is this processed and stored without any checks, or are there safety systems in place?

Big Data

13. Does the company use incoming data to produce any new insights which could improve production or service?
14. Where and in which way is this data stored?

Framework

15. Would you be able to implement the information security for Industry 4.0 technologies like Internet of Things, cloud solutions and Big Data faster and better using an information security framework specifically aimed at those technologies, compared to standard information security frameworks?
16. Is there any need for such a framework, from you and in your environment?

Note. Not all questions were asked in case a technology was not used, or if the interviewed participant had no knowledge about the subject.

Table A8

Prepared questions for semi-structured interview with colleagues at Baker Tilly.

1. Do you have (a) specific company/companies in mind for the subject of this interview?
2. In which industry does this company operate?
3. What was the state of IT and information security in this company, both for personnel and vision of the directors?
4. What was the state of Industry 4.0 implementation? Which technologies were considered or implemented?
5. Were these technologies implemented using a certain information security framework, or was the information security based on intuition?
6. What was the reasoning for this choice?
7. Were there any blockades which halted the process?
8. Would this company be interested in a framework specifically created for information security in manufacturing SMEs wanting to implement Industry 4.0 technologies? The framework is focused on being a baseline for information security.

Note. Not all questions were asked in case a technology was not used. Questions were asked multiple times if multiple companies or industries were discussing separately.

Table A9

Framework before revision

This is a baseline information security framework created with the focus on the implementation of Internet of Things, cloud solutions and Big Data. The targeted businesses for which this framework is created are SMEs in the manufacturing industry with the ambition of implementing Internet of Things, cloud solutions and/or Big Data.

This framework consists of 57 measures, each addressing an element of information security based on the so called 'CIA Triad'. This CIA Triad consists of confidentiality, integrity and availability.

The first part of the CIA Triad, confidentiality, concerns itself with the protection of sensitive information. Meaning that in every scenario, information is secure and only accessible to individuals who are authorized to do so.

The second part of the CIA Triad, integrity, concerns itself with maintaining the consistency, trustworthiness and accuracy of data over its entire lifecycle.

The third and final part of the CIA Triad, availability, deals with the guarantee that there is consistent access to all information according to specifications.
Each one of these parts are split into further aspects which contain a number of measures which together ensure the control of those aspects.

In the second table, an overview of the elements of the Internet of Things, cloud services and Big Data are shown, together with an explanation for that element, and it's appropriate important/ relevant measures. These measures can directly be referenced back to the first table using the numbers.
Internet of things can be described as a network facilitating the connection between interrelated computing devices or other 'things' able to transfer data over a network without any form of human interaction. This does not mean that human interaction is not possible. A smart thermostat, for example, can be used as an interface to facilitate human interaction. The measures for the Internet of Things are split into four layers; sensing layer, network layer, service layer and interface layer. Each of these are briefly explained in table 2.
Also known as cloud computing or cloud services, cloud solutions are internet-based IT resources. The IT resources can be requested on demand from cloud service providers. Unlike on-site IT resources, these cloud solutions are able to scale up or down quickly and on demand in order to meet business needs. This ability to meet demand is why using cloud services alongside an IoT implementation can be very valuable to the cloud user due to the flexibility of the cloud service and its cost. This is why this framework recommends the use of cloud services when implementing an IoT system. Depending on if the business uses an IaaS, PaaS or SaaS cloud service, different elements will need to be managed by the business. This can also be seen in table 3.
Furthermore, cloud solutions can be split into public clouds, private clouds and hybrid clouds. A public cloud is a cloud which is partitioned into multiple parts, which are then distributed to multiple cloud-users. A private cloud is a cloud which is dedicated to a single user or user group. Finally, a hybrid cloud is either a mix of a private and public cloud, or a combination of multiple similar clouds. This configuration provides the possibility to move applications and data from a private cloud server to a public cloud server, or vice versa, depending on the needs. This can be done as a security consideration to, for example, only keep critical data in the private cloud.
Big Data refers to a dataset which is not able to be processed by traditional tools or methods. Big Data can also be described using the three V's; Volume, Velocity, Variety, which are all high/large when dealing with Big Data. This means that the volume of data is large, the velocity (speed at which it needs to be handled) is high, and variety (different data formats) is large.

The measures describe a goal which needs to be achieved business or business layer wide. As every business is different, the measures may need to be slightly adapted to fit the applications, servers or users. Some measures have examples of implementations added, which give the business advice to the practical implementation of the measure.
The measures are described in a way most people interacting with IT are able to understand them, without needing to be tech-savvy.

For the implementation of cloud solutions, the measures are split according to the specifications in table 3. Depending on the type of service (IaaS, PaaS, SaaS), measures will either need to be implemented by the business directly, or be implemented by the service provider. In the case the service provider needs to implement the measures, a service level agreement (SLA) will need to be formulated containing the security requirements of the business based on the appropriate measures. The business will then have to (in)directly assure that these measures are actually implemented correctly, as described in measure 35.
For the use of a public, private or hybrid cloud service environment, there are no differences in this framework. Depending on the sensitivity of data and type of cloud environment, the relevant measures may be differently implemented. For example, a public cloud service environment may be assessed more on privacy towards other users of the same cloud server than a private cloud, which is dedicated solely towards a single business.

Confidentiality			
Access control	1	Establish and maintain an inventory of accounts.	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

	2	Use unique passwords.	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.
	3	Centralize access control.	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.
	4	Train workforce members on authentication best practices.	Example topics include MFA, password composition, and credential management.
	5	Select a quality password.	Make users create a password not easily guessed by using user related information. (e.g., names, telephone numbers and dates of birth)
	6	Avoid keeping a record.	Avoid users keeping a record of their passwords, unless this can be stored securely in an approved method. (e.g., password vault on phone)
	7	Avoid sharing business and private passwords.	Avoid users using a password for both business and personal use.
	8	Change first password.	Force users to change the first password the user is given.
	9	Manage default accounts on enterprise assets and software.	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
Encryption	10	Encrypt data on end-users' devices.	Encrypt data on end-user devices containing sensitive data.

	11	Encrypt data on removable media.	Encrypt data on removable media.
	12	Encrypt sensitive data in transit.	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).
	13	Encrypt sensitive data at rest.	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this measure. Additional encryption methods may include application layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.
	14	Train workforce on data handling best practices.	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.
	15	Train workforce members on causes of unintentional data exposure.	Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

	16	Ensure service provider contracts include security requirements.	Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, data encryption requirements, and data disposal commitments. Review service provider contracts annually to ensure contracts are not missing security requirements.
	17	Usage of encryption algorithms.	Use only standardized, currently accepted, and extensively reviewed encryption algorithms.
	18	Securely dispose of data.	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.
Integrity			
Security control	19	Configure data access control lists.	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.
	20	Establish an Access Granting Process.	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.
	21	Establish an Access Revoking Process.	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

	22	Define and Maintain Role-Based Access Control.	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.
Reliability control	23	Establish and maintain a secure configuration process for enterprise assets.	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this measure.
	24	Implement and manage a firewall on servers.	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.
	25	Implement and manage a firewall on end-user devices.	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
	26	Uninstall or disable unnecessary services on enterprise assets and software.	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

Integrity control	27	Establish and maintain a security awareness program.	Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this measure.
Audit control	28	Establish and maintain an audit log management process.	Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this measure.
	29	Collect audit logs.	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.
	30	Collect detailed audit logs.	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.
	31	Ensure adequate audit log storage.	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.

Additional measures	32	Implement digital signatures.	Implement digital signatures and add these signatures to every addition, modification or other action. This will provide an origin of the action by associating the action to a user and thus preventing deniability.
	33	Implement data fault tolerance.	Implement techniques to prevent faults in data. This can be done for example by implementing data redundancy techniques such as RAID or mirroring.
	34	Establish and maintain an inventory of service providers.	Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this measure.
	35	Assess service providers.	Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.
Availability			

Maintenance of software and hardware	36	Establish and maintain a software inventory.	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.
	37	Ensure authorized software is currently supported.	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.
	38	Address unauthorized software.	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.
	39	Ensure network infrastructure is up-to-date.	Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software. Review software versions monthly, or more frequently, to verify software support.

	40	Train workforce on how to identify and report if their enterprise assets are missing security updates.	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.
Maintenance of technical infrastructure	41	Establish and maintain a secure configuration process for network infrastructure.	Establish and maintain a secure configuration process for network devices like switches, access points and repeaters. Review and update documentation annually, or when significant enterprise changes occur that could impact this measure.
Disaster recovery plan	42	Establish and Maintain a Data Recovery Process.	Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this measure.
	43	Perform automated backups.	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.
	44	Protect recovery data.	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.
	45	Establish and maintain an isolated instance of recovery data.	Establish and maintain an isolated instance of recovery data on an independent node. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.

	46	Ensure service provider contracts include security requirements.	Ensure service provider contracts include security requirements, such as security incident and/or data breach notification and response. Review service provider contracts annually to ensure contracts are not missing security requirements.
	47	Designate personnel to manage incident handling.	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this measure.
	48	Establish and maintain contact information for reporting security incidents.	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.

	49	Establish and maintain an enterprise process for reporting incidents.	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this measure.
Access removal controls	50	Configure automatic session locking on enterprise assets.	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.
	51	Enforce automatic device lockout on portable end-user devices.	Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts.
	52	Enforce remote wipe capability on portable end-user devices.	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.

Devices on the network	53	Establish and maintain detailed enterprise asset inventory.	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.
	54	Utilize an active discovery tool.	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.
	55	Address unauthorized assets.	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.
	56	Separate enterprise workspaces on mobile end-user devices.	Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. This is to separate enterprise applications and data from personal applications and data.

Working locations	57	Require MFA for remote network access.	Require MFA for remote network access.

Internet of Things		
	Explanation	Important/relevant measures
Sensing layer	The layer which contains hardware such as sensors and actuators.	12, 15, 17, 23, 25, 26, 39, 53, 54, 55
Network layer	The layer containing physical infrastructure in support of connectivity between sensing layer and service layer.	39, 41
Service layer	This layer contains data storage and processing for the creation and management of services needed for interfacing with users or applications.	11, 13, 16, 17, 18, 19, 20, 21, 22, 24, 26, 33, 42, 43, 44, 45, 46, 47
Interface layer	This layer contains the methods for interacting with users or applications, such as APIs and interfaces.	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 14, 15, 19, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 36, 37, 38, 39, 50, 51, 52, 53, 54, 55, 56, 57
Cloud solutions		
	Explanation	Important/relevant measures
Applications	Application that runs on the server.	1, 2, 3, 4, 5, 6, 7, 8, 9, 14, 15, 16, 19, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 36, 37, 38, 39, 40, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57
Data	Databases.	10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 42, 43, 44, 45, 46, 47, 48, 49, 52, 53, 54, 55, 56, 57
Runtime	Keeping all processes running.	34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49

Middleware	Software acting as a bridge between an operating system and databases or applications.	12, 23, 26, 34, 35, 36, 37, 38, 39, 40, 47, 48, 49
Operating system	Operating system.	23, 27, 34, 35, 36, 37, 38, 39, 40, 47, 48, 49
Visualization	Creation of virtual servers, infrastructures, devices and computing resources.	25, 27, 34, 35, 47, 48, 49
Servers	A computer program or device that provides a service to another computer program and its user.	24, 34, 35, 41, 47, 48, 49, 53
Storage	Storage of data.	11, 12, 13, 16, 17, 18, 19, 20, 21, 22, 33, 34, 35, 42, 43, 44, 45, 46, 47
Networking	Linking of computers to allow them to operate interactively.	35, 39, 41, 53
Big Data		
	Explanation	Important/relevant measures
Network level	Related to network protocols and security, like distributed nodes and data.	24, 39, 41
Authentication level	Related to encryption and decryption techniques, logging and general authentication methods.	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16, 17, 19, 20, 21, 22, 28, 29, 30, 31, 50, 51, 52, 57
Data level	Relates to general integrity and availability challenges.	26, 27, 32, 33, 34, 35, 40, 42, 43, 44, 45, 46, 47
Generic types	Relates to traditional security tools and security related to the use of other technologies.	23, 24, 25, 36, 37, 38, 48, 49, 53, 54, 55, 56

Cloud solutions			
On-site	IaaS	PaaS	SaaS

Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Operating system	Operating system	Operating system	Operating system
Visualization	Visualization	Visualization	Visualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking
Legend:	Customer manages	Cloud service provider manages	