Maturity of organisational security governance

A case study at Damen Naval

Master thesis project: MOT2910

Milan Renne

Delft University of Technology

TUDelft

Maturity of organisational security governance

A case study at Damen Naval

by

Milan Renne

in partial fulfilment of the requirements for the degree of Master of Science in Management of Technology at the Delft University of Technology,

to be defended publicly on Tuesday August 29, 2023 at 12:00 noon.

Student Name	Student Number
Milan Renne	5553288

Graduation committee

Chairperson:	Prof.dr. M.J.G. van Eeten	Organisation & Governance
First supervisor:	Dr. S.E. Parkin	Organisation & Governance
Second supervisor:	Dr. G. van de Kaa	Economics of Technology and Innovation
External supervisor:	Ir. P.C.M. Zaat	Cybersecurity officer Damen Naval

Project duration:	February, 2023 – August, 2023
Faculty:	Faculty of Technology, Policy and Management, Delft
Date:	09/08/2023
Version:	2.0
Cover:	https://www.defensie.nl/binaries/content/gallery/defensie/content-afbeeldingen/actueel/nieuws/2023/04/03/aswf-ai-5_vier-schepen.jpg?download

TU Delft

Preface

When I started my graduation thesis journey in February this year, I wouldn't have guessed that it would have resulted in the thesis that lies before you. Most projects I had done so far had - in most cases - a clear beginning and end point in mind. Prior to starting my thesis people would tell me that a thesis project is just like any other engineering project on which you could apply tools and practices used in today's project management. Although I am usually very fond of this way of working, I quickly came to the conclusion that this project would be different.

In the weeks leading up to the kick-off meeting (the official start of the thesis project), I had different discussions and email exchanges with my first supervisor Simon Parkin about potential thesis topics. At the same time, Damen Naval was interested in measuring the maturity of its security governance. Trying to formulate a clear project that would be beneficial for Damen Naval, as well as having a meaningful academic contribution was the final goal. However, this soon became a balancing act between the different parties involved. My kick-off meeting left me with more questions and uncertainty than it gave me clarity on how to pursue the project further.

Although my thesis journey differed from a scoped engineering project, it did make me cope with challenges and setbacks and also tested my flexibility and perseverance. I remember the many 'heated' discussions I had with Simon Parkin about concepts, definitions and the right way forward. In most cases you were right – or at least convinced me I was 'wrong'. In some instances, I felt like I came up with something that made sense and continued to work on that until it reached a dead end again. All in all, those reality checks are part of doing research. It did remind me of a quote by Albert Einstein (or Socrates before him): *"The more I learn, the more I realise how much I don't know."*. The endless pursuit of learning and the fact that the more you know about a concept, e.g. security governance, the more complex it gets and the more questions arise, is something that I witnessed first-hand. All in all, I am pleased with the final result and I hope you enjoy reading.

Finally, I would like to express my gratitude to my external supervisor Peter Zaat for his guidance and precious practical insights based on his years of experience. Also, thank you for familiarising me with Damen Naval and involving me in your role as a security officer. Secondly, I would like to thank Simon Parkin for his role as first supervisor. Thank you for your supervision, honest feedback and for always being prepared to free up some time in your busy schedule. It goes without saying that I also want to express my gratitude to Michel van Eeten for being chair of my graduation committee and to Geerten van de Kaa for his role as second supervisor. I appreciate your feedback and advice during the kick-off and greenlight meeting. At last, my gratitude goes to everyone that was involved in the data collection for this project. Thank you to each and every one of you for freeing the time and actively participating in interviews or the group session!

Milan Renne
Middelburg, August 9, 2023

Summary

Existing research has shown that due to the increasing digitalization and the adoption of digital technologies and complex (big) data solutions, along with higher firm-level productivity, comes a growing and more dynamic threat environment. Organisations rely on data and digital environments. These environments enlarge the potential attack surface, as every end-point device or network node is a potential entry for malicious actors. The (un)intentional insider threat is also increasingly important for the protection of Intellectual property (IP) and business assets. Not only the attack surface has grown over the years, but also the consequences of security breaches have become more severe. Loss of confidentiality, integrity and availability can heavily disrupt working practices or even threaten the continuity of organisations. The stakes for organisational security have therefore never been higher. Current trends in coping with this new threat landscape are, among others, to increase oversight and ensure strict regulations, both via internal policy and external regulators. Extant literature also emphasises an increase in security spending, as well as technical measures to protect business assets.

This paper proposes a framework for determining the maturity of security governance within organisations. Security governance is concerned with the alignment of business goals on the one hand and security goals on the other hand, i.e. working productively and working securely. Good governance would mean that both business- and security goals can be reached without conflicting interests; preferably even by complementing one another. The research argues that security governance consists of more than merely technical measures and punitive oversight. It also parts from existing views about how more security (spending, measures, policies, etc,) is better and how security is predominantly addressed in isolation. Instead, security governance should be in alignment with 'the business' of an organisation. This brings forward the notion of security governance, as the alignment between security policies and business goals. Literature has found that these two concepts can often be conflicting, as more security in most cases impacts productivity. Therefore, the concept of maturity is coupled with the research. Maturity emphasises the alignment between security goals and business goals.

The research adopts both a conventional view of maturity, as well as a social view of maturity. The conventional view focuses on the effectiveness of security governance. A higher level of maturity indicates improving one or both of the pillars of governance, i.e. the contribution to business goals and security goals. This could mean working more productively/efficiently given certain security policies. Or - the other way around - working more securely whilst also doing projects efficiently. The social view focuses specifically on the way alignment between the two pillars of security governance is reached. It acknowledges that not all perceived governance problems in organisations have a single solution that can be imposed top-down. Instead, employees in organisations have to cope with different challenges and perceive issues related to security governance differently. The social view on maturity therefore argues that dialogue is required between a representative stakeholder group, with different viewpoints and expertise, whereby policies are drafted in concordance.

By means of a case study at Damen Naval - a large Naval shipbuilding organisation relying heavily on IP and bound by strict regulations - input was gathered regarding security governance in three individual security fields: 'access control', 'data classification, and 'monitoring & incident response. Incorporating results from a literature review, individual interviews and a focus group session, a framework was built with both a conventional assessment of security governance and a social aspect of how the alignment of policies (security- and business-related) can best be reached. The foundation of the framework consists of six dimensions of security governance:

1. Organisation-wide security and responsibility/accountability
2. Risk-based approach
3. Direction of acquisition and commitment of resources
4. Conformance with internal and external requirements
5. Security positive/conscious culture
6. Security performance measurement/alignment

These dimensions were used to guide and structure the individual interviews and led to a list of performance indicators. Each indicator steers on improving security (in terms of policy-setting) and/or productivity (in terms of contribution to business goals). The research showed that although the security fields were different from each other, most indicators could be applied to all the security fields, showing that the indicators are generalisable to an organisation-wide level. The indicators led to practical recommendations for security governance at Damen Naval. The most important takeaways are to better empower engineers in making decisions on data classification, as currently engineers feel uncomfortable in doing this due to the negative consequences of 'under classifying', which leads to information being classified higher rather than lower. Also, performance expectations should be clear for employees and additional hours spent on dealing with security measures should not be absorbed by engineers. In line with this, more effort should be put into quantifying the total costs of imposed security measures, both direct and indirect. This will make current security policies better explainable or address issues that need to be improved.

The final stage of the research aimed at reaching concordance on security governance. This was researched via a focus group session in which the metaphor of a doctor-patient relationship about a negotiated treatment plan was used to see whether and to what extent this relationship would be possible in an organisation such as Damen Naval. Despite the fact that such a relationship is hard to pursue in a large organisation with multiple stakeholders as well as being limited in autonomy due to external legislators, the results indicate that concordance would be possible, although on different levels inter- and intra-organisational. Intra-organisational, this research suggests composing an organisational structure wherein employees of the business, ICT and security are represented to discuss matters that are related to security. The focus group session itself proved that this contributed to reaching alignment. Inter-organisational, dialogue with external regulators should be pursued. Using the framework for security governance and the security performance indicators, potential misalignment can be determined systematically and a more comprehensive discussion can take place. Finally, future research could focus on improving the framework to enable a Capability Maturity Model (CMM) approach and to conduct a similar case study with the inclusion of an external regulator.

Contents

Preface i

Summary ii

Nomenclature viii

1 Introduction 1
1.1 Background 1
1.2 Research problem 2
1.2.1 Scientific contribution 2
1.2.2 Practical significance 3
1.3 Research objective 3
1.4 Research questions 3
1.4.1 Central question 3
1.4.2 Sub-questions 3
1.5 Damen Naval 4
1.5.1 About the organisation and its business goals 4
1.5.2 Why Damen Naval 5
1.6 Fit with MOT 5
1.7 Outline 6

2 Literature review 7
2.1 Key concepts 7
2.1.1 Security 7
2.1.2 Security governance 8
2.1.3 The conventional view on mature security governance 9
2.1.4 The social view on mature security governance 9
2.2 Dimensions of organisational security governance 10
2.3 Maturity models for security governance 15
2.3.1 Common characteristics of maturity models 15
2.3.2 Maturity models for the security domain 16
2.3.3 Maturity models for security governance 17
2.3.4 Limitations of current CMM approaches 18
2.4 Trade-offs in security governance 19

3 Theoretical framework 21
3.1 Compliance versus concordance 21
3.2 Misalignment and trade-offs in security governance 22
3.3 Misalignment and the effect on compliance 23

4 Methodology 25
4.1 Research strategy 25
4.2 Case study design 25
4.2.1 Unit(s) of analysis: chosen security fields 26
4.3 Data collection 27

4.3.1 Individual interviews 28
4.3.2 Focus group meeting 29
4.4 Data analysis 30
4.5 Quality assurance 31
4.6 Ethical governance, confidentiality and data management 33

5 Results 34
5.1 Security governance dimensions operationalised 35
5.1.1 Organisation-wide security and responsibility/accountability 35
5.1.2 Risk-based approach 36
5.1.3 Direction of acquisition and commitment of resources 38
5.1.4 Conformance with internal and external requirements 40
5.1.5 Security positive/conscious culture 44
5.1.6 Security performance measurement/alignment 46
5.2 Security governance performance indicators 47
5.2.1 Overarching indicators 47
5.2.2 Access control 50
5.2.3 Data classification 51
5.2.4 Monitoring & Incident response 51
5.3 On the road to concordance 52
5.3.1 Data classification 52
5.3.2 Access control 55
5.3.3 Conformance to requirements 56
5.3.4 Doctor-patient relationship applied to Damen Naval 57
5.4 Converging towards a framework for determining the maturity of security governance 58

6 Discussion 60
6.1 Major findings and their relation to theory 61
6.1.1 Issues related to security governance 61
6.1.2 Performance indicators 63
6.1.3 Concordance 66
6.2 Reflection, limitations and future research 68

7 Conclusion 69
7.1 Recommendations for Damen Naval 70

References 72

A Overview interview questions 79

List of Figures

2.1 CMM design . . . 16

4.1 Relationship between data collection methods and their contribution to the research questions . . . 28
4.2 Example of codes in audio file interview . . . 31

5.1 Left: clean picture of an F126 frigate [8], right: infographic of F126 frigate [17], both publicly available . . . 54
5.2 Developed framework for determining the maturity of security governance . . . 59

List of Tables

2.1 Existing approaches to security governance dimensions 13
2.2 Similarities of security governance domains to ISO27014 14

4.1 Data collection for individual research questions 27

5.1 Security governance dimensions used to analyse interview findings 35

A.1 Introductory and overarching interviewee questions 79
A.2 Specific interview questions on access control 80
A.3 Specific interview questions on Data classification 80
A.4 Specific interview questions on Monitoring & Incident response 81

Nomenclature

Abbreviations

Abbreviation	Definition
CBA	Cost-benefit Analysis
CMM	Capability Maturity Model
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
CAD	Computer Aided Design
CRM	Customer Relationship Management
CPS	Cyber-Physical System
DSG	Damen Shipyards Group
DSNS	Damen Schelde Naval Shipbuilding
ERP	Enterprise Resource Planning
IoT	Internet of Things
IP	Intellectual Property
IT	Information Technology
MOD	Ministry of Defense
MOT	Management of Technology
OT	Operational Technology
PDAL	Product Drawings and Associated Lists
SOC	Security Operations Centre

Key terms

Term	Definition
Security	The protection of business assets and people against harm [11].
Security governance	The alignment between security policies and business objectives of an organisation [2].
Maturity (conventional)	*”A very advanced or developed form or state.”* [21]
Maturity (social)	State of human development in which socially mature indicates a higher degree of conscientiousness, responsibility and agreeableness [58].
Compliance	Obeying a set of rules or (organisational security) policies.
Concordance	A negotiated policy among all representatives of the organisation, which is drafted in dialogue and with multi-actor expertise, instead of being mandated by a single actor (e.g. the security department) [66, 4].

1 Introduction

1.1. Background

The World we live in is rapidly changing. This line of text could have been used 100 years ago and still be true. However, the fast-paced changing environment of today, driven by digitalization, truly shapes a 'new' society beyond comprehension.

The past decades have seen a rapid rise in digitalization, i.e. the phenomenon of adopting digital technologies in business and society [5]. One way to characterise digitalization is by the number of connected devices to the Internet of Things (IoT). Even though estimates of the number of IoT devices differ, it is expected that in 2030 over 25 billion devices are connected worldwide [41, 36]. This is a 300% increase in just a decade.

The fourth industrial revolution, the IoT and big data are disruptively changing the way we live and the way products and services are designed, manufactured and distributed [73]. Digitalization within organisations is associated with higher firm-level productivity in multiple areas by enabling, improving and transforming business operations through the use of digital technologies and extensive digitised data [27, 5]. Examples of this are high-speed internet and Computer Aided Design (CAD), as these have boosted productivity within organisations. Furthermore, The utilisation of Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) have changed both the magnitude and the direction of data flows [27].

Organisations tend to embrace the potential of digitalization, as productivity growth (in)directly drives economic growth [65]. Estimates are that 49% of the world's stored data will reside in public cloud environments by 2025, with the global data sphere growing from 22 Zeta-byte (ZB) in 2018, to 175ZB in 2025 [57]. Flexibility is also an important factor. Working from home has never been easier with cloud access and centralised data storage, making it possible for employees to access data from multiple devices on demand [27]. A digitalized business landscape thus characterises increased productivity and flexibility.

The other side of the coin, however, is that digitalization has far-fetched consequences for the protection of Intellectual Property (IP) and (physical) business assets in general. At the same time as data and the transfer from endpoint devices to cloud environments have been growing, cyber threats to these business assets are increasing as well [16]. Information Technology (IT) security incidents can result in considerable costs due to data loss or system failure, but also indirect costs. One of which being reputation loss [31].

1.2. Research problem

In light of the increasing digitalization and intertwined physical and cyber environments, the stakes for security incidents in organisations, either malicious or unintentional, have never been higher. Cyber-physical attacks can have far-reaching consequences on an organisation but also on society [55]. Cyber-physical attacks on organisations may result in a number of negative business impacts. These include denial of service of computers, theft of intellectual property (IP) and sabotage of the cyber-physical infrastructure [15], resulting in loss of confidentiality, integrity and availability. Cybersecurity risks do not only come from malicious external adversaries. The 'insider threat' is just as important to consider [14]. This can both be unintentional mistakes from employees but also malicious acts from within the companies' boundaries [14].

In recent years, security spending has seen a steep rise to try and cope with the increased threat landscape [28]. Chief Information Security Officers (CISOs) have been appointed by many corporations and procedures and regulations are more strict than ever before [35]. Organisations are also bound by regulators and government agencies, as they have become increasingly punitive in their oversight of security breaches [16, 31].

Against the background of the heightened awareness of the repercussions of security breaches, organisations seem to prioritise the security of business assets above all else. Security governance, then, is skewed heavily towards the contribution to security goals instead of the alignment between business and security goals. But do all these measures yield the expected results? The impact these measures have on the productive work of employees within an organisation or the social challenges and trade-offs these measures bring forward are often overlooked. This begs the question of whether spending more, implementing stricter regulations and increasing punitive oversight is the right way forward for mature security governance.

There have been attempts at understanding and measuring the security governance of organisations. Most approaches, however, emphasise security policies, i.e. a (set of) document(s) of how an organisation plans to protect its business assets. All the same, it is possible that effective security governance entails more than only a plan with a set of security measures. Due to the greater connectivity and more complex threat landscape, security comprises more than technical solutions or procedures. It requires an extensive policy that is aligned with and supported by 'the business', i.e., an organisation's core departments/activities aimed at delivering products and making profit.

1.2.1. Scientific contribution

The scientific contribution this research aims to make is to realise a more holistic view on security governance, by developing a framework for measuring the maturity of security governance within an organisation. Execution of the framework will facilitate organisations in measuring their security governance performance and how business goals are aligned with security goals. The framework will also focus on how alignment between these two pillars of security governance can best be achieved from a social perspective. This parts from existing maturity frameworks of security governance, as these emphasise technical and organisational measures.

1.2.2. Practical significance

Some industries have a higher risk profile as security breaches have more severe consequences on the organisation. Within the naval shipbuilding industry, IP is a valuable asset, setting a competitive position and guaranteeing a firm's licence to operate. Espionage, (cyber)attacks and eavesdropping can harm the competitive position and thereby the continuity of a firm. Heavy regulations bind Damen Naval. The company has its own security policy to ensure integrity, confidentiality and availability of employees, information and assets [63]. Damen Naval is also very dependent on the work of engineers to develop ships. Employees need to be empowered to work to the best of their ability. In order to assess to what extent the security policy is aligned with business goals and the successful delivery of ships, Damen Naval wants to measure if their security governance facilitates both optimised security and contribution to business goals. It hopes to determine where their weakest links are in terms of security governance. Based on data on employees' thoughts on working practices, trade-offs they perceive in business and security and issues with current policies related to individual security fields, consensus can be reached on how to move forward and further improve governance within the respective fields.

1.3. Research objective

This research aims to design a framework, i.e. a fundamental structure, for determining the maturity of security governance within an organisation. The framework considers maturity both from a traditional role of maturity, as something that is very advanced and developed, as well as from a socially mature perspective. The former focuses on improving either or both of the two pillars of security governance: security policies and contribution to business goals. The latter perspective emphasises that maturity is concerned with the way how alignment between the two pillars is sought. During the design process of the framework, this research aims to gather valuable insights about mature security governance and its trade-offs or (mis)alignments, from employees at Damen Naval.

1.4. Research questions

1.4.1. Central question

What is a suitable framework for determining the maturity of security governance within an organisation?

1.4.2. Sub-questions

The sub-questions below help structure the research and facilitate answering the central question. Sub-question 1 and 3 focus on the conventional maturity of security governance, whereas sub-question 4 addresses the social maturity of security governance. Sub-question 2 aims to give an understanding of existing trade-offs in security governance from theory, complemented by the challenges that employees at Damen Naval perceive.

1. What are useful dimensions along which security governance can be assessed?
2. What are trade-offs related to security governance within an organisation?
3. What are suitable indicators for security governance of security fields at Damen Naval?
4. How can concordance be reached on trade-offs regarding security governance at Damen Naval?

1.5. Damen Naval

1.5.1. About the organisation and its business goals

Damen is a third-generation shipbuilding family business with its small beginnings in 1927 when brothers Jan and Rien Damen started a small yard in Hardinxveld, the Netherlands [30]. A lot has changed since then. From 1969 onwards Damen introduced standardised shipbuilding and in the 80's it set its goals on the global market [30]. It acquired Royal Schelde (founded 1875) in the year 2000, marking the official start of Damen Schelde Naval Shipbuilding. The whole Damen Shipyards group consists of 55 companies and 35 shipyards worldwide, with a turnover of 2.5 billion euros in 2022. Yearly, Damen delivers over 175 ships and its current employee count is 12.000. Around 1200 of those employees work for Damen Naval. Damen Naval is the naval shipbuilding division of the Damen Shipyards Group, building and integrating a variety of Naval ships, ranging from frigates and large custom support ships, to patrol vessels and RHIBs.

Damen Naval has its launching customer in the Royal Dutch Navy. This means that Damen Naval closely cooperates with the Dutch Navy and the Ministry of Defense (MOD) to develop and build innovative projects. The relationship between the Royal Dutch Navy and Damen Naval is of strategic importance for its continuity. Damen Naval also delivers to EU/NATO navies and projects outside the NATO/EU frame [18].

Over the past years, the order intake for Damen Naval was lagging. One of the reasons for this was the budget cut by the Dutch Government in the Navy, preventing any orders from the Dutch Government for over 10 years. Also, the aggressive international campaign of French state-owned Naval Group to become the naval shipbuilding leader in Europe sets Damen Naval in a difficult position. Currently, the order intake and expected projects give a positive take on the near future [18]. However, Damen Naval needs to carefully select a limited number of opportunities that contribute to a long-term strategy, as well as understand that the Dutch MOD is a customer to be conquered and not some actor to whose orders Damen Naval is entitled without a good sales approach [18].

In its business plan, Damen Naval formulated a vision and mission, accompanied by a set of goals for the coming years. Their vision, in short, is to be a leading provider of naval vessels. What the organisation does, today, to become this leading provider of naval vessels, is described by their mission:

> Damen Naval is a client-focused, internationally operating division... We design, engineer and (manage to) build innovative combatants, auxiliaries and co-design and co-build expeditionary submarines of excellent quality. Our clients are governments and navies from around the world. We strive to exceed our clients' expectations in terms of quality, innovation, reliability and life cycle costs. By serving the needs of our clients worldwide and every day, we fight to become a leader in the open export market for combatants. [18] (p. 9).

This mission requires Damen Naval to deliver ships on time and within budget, with shorter project delivery times than the competition and manage the integration of the ship's platforms and systems [18]. It is also worth mentioning that Damen Naval is prioritising quality over (direct) costs. Due to the quality of its ships, overall lifecycle costs might be lower, but it is not directly competing on list price.

1.5.2. Why Damen Naval

Related to the organisation's goals and mission statement, it is no surprise that Damen Naval relies heavily on the protection of its assets and IP, as it strives for quality and innovation. The confidential nature of the products that are made makes Damen Naval an interesting organisation to conduct a study about security governance. Also, the organisation is bound by heavy regulations that result in strict policies and security measures. These regulations and policies have consequences on the labour force as well. A heavily engineering-dependent organisation like Damen Naval wants to focus on its engineering practices, but because of the strict regulations and complex threat landscape, there are wicked challenges in terms of security governance.

Another major reason for choosing Damen Naval as a focal company for the research is the significant growth of the organisation over the past few years. Due to the increased order intake and future prospects of large and complex projects, Damen Naval is attracting more engineers and specialists. The sudden growth and requirements for working on complex projects, resulted in Damen Naval changing its way of working by implementing separated working environments (standard and restricted), as well as a variety of IT- and engineering tools, such as a PLM (Product Lifecycle Management) platform. The sudden growth, coupled with a radical change in the working environment, results in even more challenges for the organisation to undertake. Security policies need to be updated and aligned with the practices of 'the business'. A preliminary exploratory analysis of the organisation showed that employees perceive security measures as restrictive in conducting their own work. Key issues are the implications to data classification, the restrictive access control policies and the separated working environments. The organisation thereby faces a continuous balancing act between working productively and working securely.

1.6. Fit with MOT

The Master Management of Technology (MOT) at the Faculty of Technology, Policy and Management of the Delft University of Technology aims to teach students how to use technology as a corporate resource. Many of the upcoming technologies in today's society are driven by digitalization. Therefore, understanding how to best protect these technologies, is an increasingly important aspect of managing technologies. On top of that, the chosen topic of security governance is also dependent on many different factors and stakeholders, which matches nicely with the interdisciplinary nature of MOT.

The course inter- and intra-organisational decision-making introduced me to the concept of 'wicked problems'. Wicked problems are characterised by having no straightforward right/wrong answer or a 'best' solution. These problems are multi-stakeholders with conflicting agendas and fading boundaries of disciplines and organisations. This course taught me to look at a problem from multiple perspectives, e.g., from an engineer, a security officer and a manager. It also showed how making purely rational or objective decisions can be troublesome, as the perceptions of stakeholders are important to take into account as well. This was specifically important for the case study at Damen Naval. Finally, the need to evaluate trade-offs of conflicting objectives was one of the motivations to engage in the research project.

Another course that fits well into the research is the course 'leadership and technology management'. This course considered the topic of organisational change and the factors that influence this. Security governance also relates to organisational change, because it takes into account the whole organisation and requires the support of all stakeholders involved. On top of that, the first part of the course, about the knowledge economy and the change of organisational structures to be more dependent on ICT, made me realise how important a correct adoption of digital technologies within organisations is. This also made me more aware of possible negative consequences of ICT, such as cybersecurity risks, which was one of the drivers for me to pursue this specialisation track.

Although the specialisation track is not part of the key courses of MOT, it is one of the key tracks for the specialisations of studies at TPM. The specialisation of cyber security aligns perfectly with the research. I took a great deal of inspiration from the following courses during this specialisation. The course 'user-centred security' taught me, among other things, that 'the user (or employee) is not the enemy' and that policymakers, as well as security managers, should make the policies in such a way that it aligns with the primary tasks of employees, as adhering to security measures is mostly not without costs. This also led me to pursue the concept of security governance as a more comprehensive alignment between productivity and security.

1.7. Outline

Chapter 2 of this report defines key concepts used in the research and explores dimensions and maturity models of security governance. It also discusses how security and productivity is weighed, as well as other trade-offs in security governance. The theoretical framework of chapter 3 provides a lens for the framing and interpretation of the research results. Next, a comprehensive overview and argumentation of the research design is given (chapter 4), followed by the results section in chapter 5. The results include the analysis of the individual interviews and the extracted security governance performance indicators. The analysis of the focus group session is presented afterwards. The results section ends with a visualisation of the framework and a short description. The results section is decoupled from the interpretation of the results, which is discussed in chapter 6. The discussion chapter also mentions some limitations of the study and proposes a few directions for future research. The final chapter presents the overall conclusion and gives recommendations for Damen Naval to improve its security governance.

2

Literature review

This chapter presents the literature review for this research. First, the key concepts of this study, both delineated and in relation to one another, are carefully defined in section 2.1. Next, dimensions of security governance are explored based on a comparison of previous literature reviews, as well security governance frameworks and ISO standards, with the aim of extracting dimensions for security governance to base the maturity protocol on (section 2.2). Chapter 2.3 defines what maturity models are and explores extant literature on maturity models for security governance. The section also relates the definition of maturity from section 2.1 to existing maturity models, to understand if there are applicable models available.

2.1. Key concepts

2.1.1. Security

Security - and its derivatives - is a term widely used in literature, but its definitions and interpretations of what constitutes security vary widely. Dictionaries do not even agree with the definition of the basic notion of security [61, 21]. What most definitions have in common is that it entails the protection of someone or something against harm or non-desirable outcomes. Security and safety are also frequently mistaken for each other. Security is concerned with harm due to intentional acts whereas safety is the protection against unintended risks.

The basic notion of security does not distinguish what is to be protected against harm. This can be a person, organisation or object, both physically and digitally. On top of this basic definition, security is always involved in some sort of risk or threat assessment, in order to determine the level of protection against harm. In recent years, many derivatives of security became popular, such as cyber security and digital security. According to Cisco [13] *”Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks”* (’What is cybersecurity’, para 1.). Comparable definitions are given by online dictionaries, as well as scientific literature [25, 11].

These definitions might seem to narrow down what security constitutes, but in today’s highly digitalized cyber-physically converged society, this is not the case anymore [11]. Mullet, Sondi, and Ramat [52] argue that cybersecurity is not limited to technical subjects and is not only applicable to the IT domain. Their research states that:

- Cybersecurity involves all stakeholders within and across companies, not only the IT department [52].

- Cybersecurity is not restricted to the virtual world, but has involvement of the physical world by humans and physical infrastructure [52].

Considering the additional propositions of cybersecurity by Mullet, Sondi, and Ramat [52] and the consensus on definitions by Cains et al. [11], the definition of security as protecting someone or something against harm or non-desirable outcomes is still relevant. For organisations, 'the something' can be defined as 'business assets' and 'the someone' will comprise employees and clients, as well as other people that may be affected by harm. Harm to business assets can be a variety of things: loss of money, downtime of machines or IT/OT infrastructure [15, 55]. Business assets in today's era are attacked more and more via 'the someone', therefore making the protection of employees vital for business continuity.

Harm to business assets may result in an organisation losing the confidentiality of IP and being deprived of its license to operate due to loss of reputation. For our definition, the discontinuity of business is the greatest harm to an organisation. However, one could argue that even greater harm would be the impact on society as a consequence of losing IP or an attack on business assets in general. 'the someone' in the definition, therefore, also comprises people impacted by attacks on an organisation. To conclude, the definition of security for this research is *the protection of business assets and people against harm.*

2.1.2. Security governance

Governance, in general, is *"the act or process of governing or overseeing the control and direction of something"* [49]. Applied to security, this would mean: overseeing the control and direction of protecting business assets and people against harm. Despite the fact that this is a clear and understandable definition of security governance, existing literature has different interpretations of the term.

In the past, security governance was seen more as a subset of IT governance, with a focus on technical details and - often - obstructive security controls that hampered business productivity [60, 2]. This tends to neglect the modern security governance definition of alignment with security policy and business objectives [2].
In order to steer away from this subset of IT governance definition, Schinagl and Shahim [60] covered some key areas of 'improvement' over traditional security governance:

1. continuous and resilient approach to security instead of a preventive approach;
2. collaborative top-down security function, instead of bottom-up isolated security;
3. supportive of business innovations instead of obstructive security controls;
4. board commitment over operational security;
5. governance is focused on business risks that impact strategy, instead of a focus on technical details [60].

In line with the areas mentioned above, security governance is best defined as the alignment between security policies and business objectives of the organisation [2], instead of merely overseeing the control and direction of business assets, arguably mostly done from an IT perspective. According to this definition, both the security policy and the business objectives of an organisation need to be defined and understood, before alignment can take place. The security governance structure is unique for every organisation [51]. Depending on the specific business objectives and the security policy of an organisation, specific security governance objectives and dimensions can be derived.

The security governance areas in the list by Schinagl and Shahim [60] also include a top-down approach as well as top-management engagement, with security governance seen as a strategic issue, rather than just the responsibility of the IT department [43]. Be this as it may, these points were only included to give a better understanding of how modern security governance is or preferably should be executed. The improvement areas are not considered part of our basic definition of security governance, as adding adjectives to the basic definition only hints at what constitutes 'good' security governance.

2.1.3. The conventional view on mature security governance

Both Mettler, Rohner, and Winter [50] and Lasrado, Vatrapu, and Andersen [46] use the following definition by the Oxford dictionary of 'maturity' in their respective papers: *“the state of being complete, perfect or ready”* [50] (p.334). At first sight, this might look like a probable definition of the term. However, being complete and perfect is very hard to achieve in practice and only strived for in real-life situations.

To make this clear, consider the coupling of maturity with security. Given the basic definitions we proposed thus far, combining maturity with security would mean as much as 'the complete and perfect protection of business assets and people against harm'. This would mean that mature security would be perfect in the sense that business assets and employees are completely protected against harm. In its turn, this could imply that no more risk is left as perfect protection would theoretically indicate a zero possibility of harm.

In addition to the discussion that one could argue if 'zero-risk' is even possible [12], another important factor is that realising (near) zero-risk is costly and directly affects other practices, such as usability and productivity. This is usually described as the ´security trade-off' and is closely related to security governance.

Maturity is better characterised by *”a very advanced or developed form or state”* [21], instead of something that is 'perfect' and 'finished'. Mature security would then relate more to the continuous development of security, which is in line with a definition by Cains et al. [11]. Mature security governance, in its turn, would relate to the continuous development or improvement of either or both business goals and security policies. Governance is then improved, if, for example, security policies are improved upon without hampering the productive flow of employees within an organisation. The other way around, governance is improved if working practices are made more productive without this negatively affecting security policies. This definition can be considered as the 'conventional or traditional' way of looking at maturity. It entails advancing and improving but acknowledges that a 'perfect or complete' state may never be reached considering the complexities underlying security governance and the state of uncertainty.

2.1.4. The social view on mature security governance

Another view on mature security governance is more socially oriented. This view acknowledges that for wicked problems and highly complex topics, maturity is not so much about finding the absolute truth or a perfect solution. Instead, it emphasises social relations and stakeholder dialogue to consider expertise and opinions that build up towards a supported optimised solution.

Within an organisation, maturity for security governance is about being able to discuss openly what the 'right' way forward is for an organisation and how the security policy best aligns with the business goals. This might impact an individual department or employee more than it would impact someone else, but overall consensus has to be reached on what is the most beneficial for the organisation as a whole. The maturity of humans can be a perfect metaphor for this line of reasoning, as with age, people become more conscientious, responsible and agreeable (socially mature). Compared to infants, adults can make more informed decisions and arrive at a consensus about conflicting interests more easily [58]. Just like society expects adults to come to a consensus in discussions more easily than infants, the same applies to maturity within organisations.

Within organisations, different employees, with different roles and from different departments, all have their own priorities and objectives. Overall, their objectives (hopefully) contribute to the business goals of an organisation. However, more often than not, business objectives can conflict.

> *”Systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail”* [3] (p.610).

This quote by Anderson and Moore [3] explains how the lack of ownership over a problem and misaligned incentives can result in ’failed systems’. Even though this statement originates from industry, the same is applicable to the boundaries of a single organisation. Incorporating expertise and input from a representative stakeholder group may prevent these ’failed systems’ and therefore contribute to socially mature security governance. The highest notion of social maturity for this research is achieved when concordance is reached in the alignment of security policies and business objectives. Contrary to compliance, concordance aims to achieve a negotiated policy among all representatives of an organisation, drafted in dialogue and with multi-actor expertise, instead of being imposed upon a single actor (group), such as a security department.

2.2. Dimensions of organisational security governance

In order to come up with a framework for measuring the maturity of security governance, direction is needed as to what it is that is measured. A firm’s governance structure is or should be unique to its objective and performance goals, as was discussed earlier in the definition of security governance. Be this as this may, organisational security governance usually comprises similar dimensions and fundamental objectives. This chapter aims to derive these fundamental dimensions and objectives. It builds upon previous literature reviews related to security governance dimensions by Mishra [51] and AlGhamdi, Win, and Vlahu-Gjorgievska [2].

Extant literature consists of a wide variety of security governance frameworks, best practices, models and objectives. It is worth mentioning that there are a number of overarching (information) security standards, norms and frameworks available within the industry. The most renowned are COBIT 5, ISO/IEC 38500 and ISO/IEC 27014 [72]. ISO 38500 is an international standard for IT governance, based on six principles [72]. It mostly sees IT as a means for meeting organisational objectives. Another renowned standard is ISO 27014. This standard is aimed more specifically towards organisational security governance of IT and is part of the ISO 2700 series. The standard hosts six individual objectives:

1. establish comprehensive (organisation-wide) information security;
2. adopt a risk-based approach;
3. set the direction of investment decisions;

4. ensure conformance with internal and external requirements;
5. foster a security-positive culture;
6. ensure security performance meets current and future business goals [39, 72].

The first objective also states in the standard that activities concerning physical and logical security should be closely coordinated [39]. This is an interesting description, as even though the standard is concerned with IT governance, the physical aspect is not overlooked. This is a pitfall of many IT security governance approaches. The second objective determines the acceptable level of risk appetite of the organisation [39]. Objective three sets the direction of acquisition, including adopting new technologies and investment activities. The fourth objective is especially important for Damen Naval, as the company is bound by strict external regulations. Objective five aims to create and maintain a security-positive culture. The final objective means that the security structure of the organisation is fit for purpose. This entails monitoring and auditing [39].

The COBIT (Control OBjectives for Information and related Technologies) framework consists of five domains. The framework is particularly useful for the alignment between IT governance and business objectives, but it lacks convergence towards security governance. However, the COBIT 5 for information security is more useful in this regard. It builds on the COBIT 5 framework but is more practical and converged towards information security. The five main domains of COBIT 5 information security are given in table 2.1. The fifth domain: the separation of governance from management, requires more context. COBIT 5's view on this is that governance concerns itself with setting the direction of a security governance framework, as well as monitoring and evaluating performance. Management is the executable branch that plans, builds and runs activities in alignment with the direction of the governance body [37]. This is in contrast to ISO27014, which doesn't mention such a separate structure. Instead, the emphasis within ISO27014 lies on implementing information security and risk management across all levels of an organisation, as a part of the overall business strategy.

AlGhamdi, Win, and Vlahu-Gjorgievska [2] extracted a number of critical success factors for an information security governance framework. These success factors were later combined into domains based on their objectives and traits. The seven domains are: 'responsibility and accountability', 'awareness', 'compliance', 'assessment (auditing)', 'measurement', 'reporting' and 'monitoring' [2]. Interestingly to note here is the definition used for compliance: *"Compliance represents a balance between the organisation's objectives and information security policies and procedures to provide the maximum level of protection for the organisation"* [2] (p. 12). This is a shift from the older definition used and implemented within organisations as the adherence of employees to the security policy. The definition by AlGhamdi, Win, and Vlahu-Gjorgievska [2] already takes alignment with business goals into consideration.

Another domain that is crucial for the research is the domain of 'measurement', as this is strongly related to the maturity of security governance. The paper even mentions how different studies have suggested techniques for measuring the maturity level of an organisation's security governance [2]. Even though no best-fit measure was proposed, security awareness, culture and employee commitment were among the most used measures for security governance maturity [2].

Mishra [51] extracted six fundamental organisational security objectives that are theoretically grounded and value-based, i.e. incorporating values of individual organisational members. The objectives are as follows:

1. ensure a corporate controls strategy;
2. establish a control-conscious culture;
3. ensure clarity in policies and procedures;
4. ensure regulatory compliance;
5. ensure continuous and iterative control assessment;
6. ensure responsibility and accountability. [51]

The security governance objectives above have much in common with the six objectives of the ISO27014 standard. Regulatory compliance is similar to conformance with internal and external requirements. A control-conscious culture has a direct relation with a security-positive culture. Also, a continuous and iterative control assessment, as well as clarity in policies and procedures, can be compared with the assurance that security performance meets current and future business goals. Finally, a risk-based approach, setting directions of investment decisions and organisation-wide security (objective 2, 3 and 1 of ISO) can all be related to a corporate control strategy (objective 1 [51]).

Gashgari, Walters, and Wills [29] propose a security governance framework based on a number of security governance success factors. These success factors were combined into a security framework of five overarching security governance areas: 'strategic alignment', 'performance measurement', 'value delivery', 'risk management' and 'resource management'. Again, all of these security governance areas can be related to the objectives for effective security governance of the previous papers. Even though the names of these security governance areas are different, the underlying security governance success factors are similar to the other dimensions discussed earlier [39, 38, 51, 2].

The final approach to security governance dimensions included in this review is proposed by Westby and Allen [68]. The paper describes eleven characteristics of effective security governance. Opposed to the other frameworks, this paper comprises of more characteristics for effective security governance. This does not necessarily mean that the level of detail is different or that the other papers/standards 'missed' essential dimensions. Most of the characteristics can be included in the dimensions of other frameworks. The characteristic 'accountability of leaders' mentions that leaders or management are accountable for security [68]. This might imply that role-accountability in other layers of an organisation is not needed. More recent studies about security governance departed from this statement and consider accountability for parts of security to be part of every employee's role [39, 2]

After careful analysis of the objectives, factors or key principles within the reviewed literature, table 2.1 was drafted to compare the different dimensions with each other. Even though some papers have addressed security governance dimensions as objectives, or vice versa, the list only comprises dimensions/factors, i.e. without describing a specific preferred state of the dimension within security governance. This led to the wording of some of the dimension being changed slightly (e.g., the objectives by Mishra [51]). At first sight, this might be perceived as altering definitions. However, the terms were changed within the context of the initial papers and their definitions remain intact. The conversion to the security governance dimensions in table 2.1 facilitated a better comparison between the domains. This comparison revealed overlap as well as support for most of the security domains.

Table 2.1: Existing approaches to security governance dimensions

Source	Security governance dimensions
27014 ISO/IEC [39]	Organisation-wide information security Risk-based approach Direction of investment decisions Conformance with internal and external requirements Security-positive culture Security performance alignment to current and future business goals
AlGhamdi, Win, and Vlahu-Gjorgievska [2]	Responsibility and accountability Awareness Compliance Assessment (auditing) Measurement Reporting and monitoring
Mishra [51]	Corporate controls strategy Control-conscious culture Clarity in policies and procedures Regulatory compliance Continuous and iterative control assessment Responsibility and accountability
COBIT 5 security ISACA [37]	Conformance with stakeholder needs Enterprise-wide security Integrated framework Holistic approach Separation of governance from management
Gashgari, Walters, and Wills [29]	Strategic alignment Risk-based approach Resource management Performance measurement Value delivery
Westby and Allen [68]	Enterprise-wide security Accountability of leaders Security as business requirement Risk management Roles, responsibilities and segregation of duties Enforcement of security in policy Level of resources committed Staff awareness Planned, managed, measurable and measured Reviewed and audited

In order to better grasp the relations between the security governance dimensions, table 2.2 was drafted. This table compares the security dimensions of ISO27014 with the other approaches to security governance. The 'x' in the table shows which individual dimensions of ISO27014 relate to the dimensions of other literature. ISO27014 was chosen as this ISO standard is most applicable for security governance principles and it is part of the ISO27000 series that is widely adopted in extant literature [2].

Almost every security governance dimension could be linked successfully to a domain of ISO20714. Three dimensions were not linked to either of the dimensions: 'Clarity in policies and procedures', 'separation of governance from management' and 'accountability of leaders'. The first dimension didn't fit any of the dimensions as it is arguably on another level compared to the other characteristics. Clarity in policies and procedures could be a characteristic of security performance alignment. Prior to alignment, clarity is needed as to what it is that is being aligned. Security performance is also dependent on the right policies and procedures. Separation of governance from management is not linked to any of the security governance dimensions, as the definition is not shared with the organisation-wide security governance approach [68, 39, 51]. Higher management should have a leading role in promoting and supporting security governance, but the separation of governance from management by ISACA [37] is not specifically agreed upon in existing literature [39, 2]. The same can be said about the accountability of leaders. Even though leaders should be accountable for security, so does everyone else within an organisation. Falling back on the paper by Anderson and Moore [3], shared accountability is needed in a good functioning organisation.

Apart from the three 'outliers' all other dimensions were coupled to the dimensions of the ISO standard quite easily. Some dimensions were straightforward to link, e.g. 'organisation-wide security'. It should be noted that dimensions like 'accountability and responsibility' were also added to this dimension, as to quote the description of the dimension by ISO/IEC [39] "*responsibility and accountability for information security should be established across the full span of an entity's activities*" (p. 5). Other dimensions had overlap between multiple ISO dimensions, e.g. 'corporate controls strategy' for 'risk-based' and 'direction of acquisition' dimensions. This can be explained by the fact that corporate controls strategy requires conducting risk assessments [51], particularly for acquisitions and investment decisions [39].

Table 2.2: Similarities of security governance domains to ISO27014

Source	**Security governance dimension**	**Similarities to ISO27014**					
		Organisation-wide	**Risk-based**	**Direction of acquisition**	**Conformance with requirements**	**Security-conscious culture**	**Security performance alignment**
27014 ISO/IEC [39]	Organisation-wide information security	x					
	Risk-based approach		x				
	Direction of acquisition			x			
	Conformance with internal and external requirements				x		
	Security-positive culture					x	
	Security performance alignment to current and future business goals						x
AlGhamdi, Win, and Vlahu-Gjorgievska [2]	Responsibility and accountability	x	x				
	Awareness					x	
	Compliance				x		
	Assessment (auditing)				x		
	Measurement						x
	Reporting and monitoring						x
Mishra [51]	Corporate controls strategy		x	x			
	Control-conscious culture					x	
	Clarity in policies and procedures	-	-	-	-	-	-
	Regulatory compliance				x		
	Continuous and iterative control assessment						x
	Responsibility and accountability	x				x	
COBIT 5 security ISACA [37]	Conformance with stakeholder needs						x
	Enterprise-wide security	x					
	Integrated framework	x					
	Holistic approach			x	x	x	x
	Seperation of governance from management	-	-	-	-	-	-
Gashgari, Walters, and Wills [29]	Strategic alignment	x					
	Risk-based approach		x				
	Resource management			x			
	Performance measurement						x
	Value delivery					x	
Westby and Allen [68]	Enterprise-wide security	x					
	Accountability of leaders	-	-	-	-	-	-
	Security as business requirement						x
	Risk management		x				
	Roles, responsibilities and segregration of duties	x					
	Enforcement of security in policy				x		
	Level of resources committed			x			
	Staff awareness					x	

In the final analysis, the explored security governance dimensions from the different sources have much in common. Even though the phrasing of individual terms may differ, most of the analysed literature on security governance addresses comparable dimensions. Overall, ISO27014 was used to compare the other selected dimensions. Based on this norm and the similarities and phrasing of the other sources, a list with the following dimensions was chosen for the key security governance dimensions for this research:

1. Organisation-wide security and responsibility/accountability
2. Risk-based approach
3. Direction of acquisition and commitment of resources
4. Conformance with internal and external requirements
5. Security positive/conscious culture
6. Security performance measurement/alignment

These dimensions of security governance are especially relevant for the further stages of the research, as they delineate what security governance comprises as well as give guidance on structuring the results of the case study.

2.3. Maturity models for security governance

2.3.1. Common characteristics of maturity models

In the extant literature, a recurring approach to measuring maturity is by utilising some form of a maturity model. Building on the definition of maturity, as an advanced or developed form or state, a maturity model would be something that identifies the level of advancement and development. It is important to note here that this definition is about maturity in general, but does not specifically align with our definition of mature security governance in chapter **??**.

Mettler, Rohner, and Winter [50] proposes six basic components of maturity models:

1. A number of maturity levels (usually between 3 and 6);
2. a descriptive label for each level such as initial, repeatable, etc.;
3. a summary on a generic level of the characteristics corresponding to the maturity level;
4. dimensions or process areas for each maturity level;
5. specific elements or operationalised constructs to be performed at each maturity level;
6. a description of these elements or operationalised constructs.

Even though these basic components give some direction to what a maturity model constitutes, plenty of maturity models have been developed over the years. Some models are more practical in nature, whilst others focus more on the normative aspect of what maturity should be [46]. In order to be able to get a better understanding of the different maturity models in existing literature, as well as being able to reuse and compare them, Mettler, Rohner, and Winter [50] came up with a classification system for maturity models (oriented at information systems). According to this classification system, maturity models are mapped based on general model attributes (such as name, addressed topic and origin of the model), the type of maturity model design and the use of the maturity model (for self-assessment, auditing or as a practical tool for development).

A research paper by Lasrado, Vatrapu, and Andersen [46] identified three basic worldviews of maturity models, that correspond with the classification system by Mettler, Rohner, and Winter [50]. The first worldview portrays maturity as a normative theory for a single focal actor to pursue a state of being mature. The second proposed worldview characterises a maturity model as a best practice guide. The third worldview of maturity models is concerned with inter-organisational bench-marking. This research would be most suited to incorporating the second worldview on maturity models, as it is not only interested in the normative aspect of maturity within an organisation, i.e. what an organisation should do to develop and advance, but also about how it is currently doing and what is needed in practice. The third worldview is not applicable to the research as this view is limited to bench-marking maturity across organisations.

The most renowned type of maturity model that adheres to the second worldview is the Capability Maturity Model (CMM). CMM originates from the late 1980s, when it was developed by the Software Engineering Institute (SEI). The widely adopted initial model of CMM consists of five maturity levels, from level 1 to level 5: 'initial', 'repeatable', 'defined', 'managed' and 'optimizing' [54]. Despite the initial model being used for software development, it was adopted by many other fields and research areas [1, 56, 69]. Based on the basic components of a maturity model by Mettler, Rohner, and Winter [50] and insights from the ISO/IEC 15504, a CMM could look like figure 2.1.

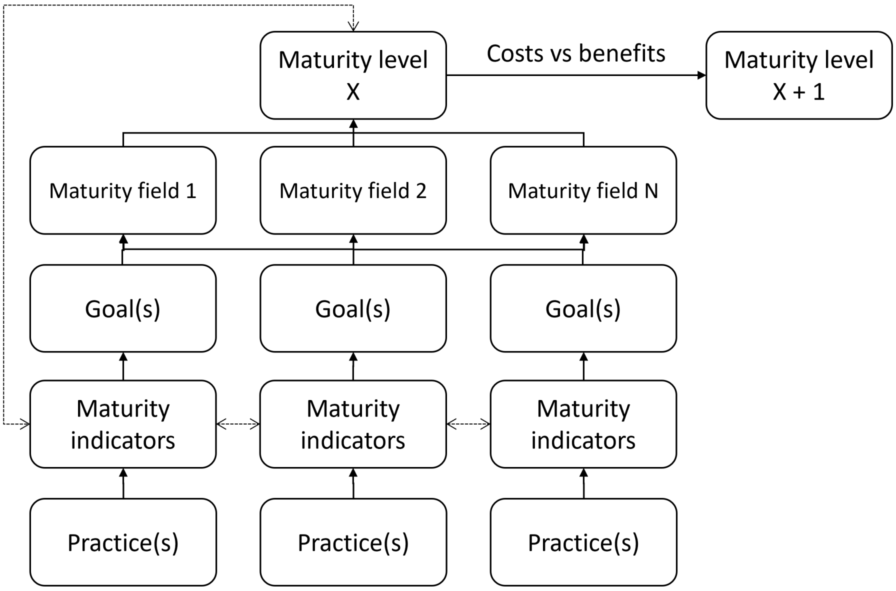


Figure 2.1: CMM design

2.3.2. Maturity models for the security domain

Despite the fact that CMM is a renowned model that has had many successfully implemented derivatives over time, the implementation in the security domain is limited [42]. Most of the CMM approaches that are adopted in the security domain are focused on the information security field. Some of the key CMM-based security maturity approaches are The Cybersecurity Capability Maturity model (CM2) [6], Systems security engineering CMM (SSE-CMM) [69], Electrical Subsector Cyber Security Capability Maturity Model (ES-C2M2) [1], IT capability maturity framework (IT-CMF) [42], Cyber Security Capability Maturity Model (CSCMM) [22] and the Cybersecurity Capability Maturity Model (C2M2) [24].

These specialised variants of the original CMM developed by SEI are useful for specific domains, but the 'source' model needs to be broadly applicable [54]. The sweet spot would be to have a broadly applicable model that is suitable for tailoring to specialised domains, e.g. a security field within Damen Naval. Let's consider the advantages and drawbacks of some of the specialised CMM approaches first.

Although building upon the initial CMM framework, CM2 is an inter-organisational model as it serves as a basis for comparative assessment across organisations and enables cross-border collaboration [6]. The goal of the model is to achieve sustainable security advantage, following a 5-factor model consisting of 'capabilities', 'technological development', 'Threats' and 'vulnerabilities'. These factors are the basis for the proposed maturity indicators. The way these indicators are filled in, describes the corresponding maturity level [6]. An advantage of this model is its comprehensive view of security, taking into account external factors and the environment as well. Also, the zero to five stages of CM2 are related to stages of human development (prenatal, infant, child, adolescent, adult and sage) [6]. This aligns with our definition of maturity. A pitfall of this approach is that the model merely hints at what a respective level would entail. On top of that, the maturity indicators are more focused towards the execution of operational and technical measures of security, as opposed to the governance thereof.

Alternatively, the ES-C2M2 is highly operationalisable but is more focused towards cybersecurity. It constitutes of 10 domains of cybersecurity, with each domain consisting of specific objectives. Each objective, in turn, comprises multiple practices [1]. What is interesting about this model is that the maturity indicators are assigned at the level of practice, instead of at a higher level. This enables measurement at a detailed level and gives much more detailed information to determine a maturity level. ES-C2M2 only utilises three maturity levels (excluding level 0). A general higher level can only be obtained if all domains are scored on the corresponding maturity level. Prior to this, all objectives for a specific domain should score the same maturity level. Before doing so, all practices for a single objective should score the right maturity level. This bottom-up approach enables practitioners to work their way up and systematically improve the maturity of an organisation.

To conclude, ES-C2M2 has many favourable characteristics and positions itself as the best-suited model for maturity capability. The structure of the maturity model facilitates high applicability to multiple security domains, and, at the same time, goes in-depth to a practice level. The only downside of this model is - in line with the other security maturity models - that it is concerned with improving the security performance of an organisation, but not necessarily with the governance, i.e., the alignment between business goals and security policy.

2.3.3. Maturity models for security governance

Opposed to maturity models for security, maturity models for security governance are expected to include alignment between business goals and security policy. However, these models are even more scarce than the security maturity models.

One of the few approaches to a maturity model for security governance is provided by Bruin and Solms [9]. The five components are: 'capability', 'contingency', 'capacity (building)', 'conformance' and 'threat'. These components together form the dashboard or overarching security governance model. Each component that is based on other maturity models is subdivided into three categories: 'people', 'processes' and 'technology'.

Subdividing into the three categories makes it easier to relate the individual components to one another. Maturity is assessed on a four-level scale. One of the benefits of this model is the comprehensive and systematic assessment of maturity, as well as integration of the 'human' side of security governance. The downside of the model is the lack of 'physical' aspects of security governance and its emphasis on cybersecurity. In another paper by De Bruin and Solms [19], cybersecurity was defined according to 27032:2012, i.e. as part of IT security. The paper does not mention any physical aspects of security, which is necessary for the research. Furthermore, the maturity levels of the 'people' category are formulated in a very high-over manner, making it difficult to apply in an organisation.

Maleh et al. [48] took on another approach to (cyber) security governance. Their capability maturity framework consists of five governance capabilities: 'Information security, governance strategy and metrics', 'technical asset security management', 'information service/system/data security management', 'vulnerability and risk management' and 'information security governance, control/compliance/continuity management'. These overarching capabilities are decomposed into 21 objectives for security governance [48]. Each of the 21 objectives is assessed based on a number of questions that result in a five-level maturity scale.

The maturity scale itself was made specifically for governance on security. It takes into account the alignment between business and IT (security), risk appetite and it includes physical environment security [48]. Compared to security-centred CMM, this maturity model is better suited for the research. Even though the top-level governance capabilities do not exactly align with the chosen dimensions of security governance of chapter 2.2, many of the objectives and the related maturity scale do fit the selection of security governance dimensions.

2.3.4. Limitations of current CMM approaches

The literature review on existing CMM approaches showed that only a few maturity models are concerned with governance, as the majority focus on security policy. Those models concerned with security policy emphasise 'technical' solutions by suggesting implementing more security measures and attaining more personnel [35]. Also, CMM approaches view security through a specific lens, mostly from an I(C)T perspective. Even though security, nowadays is much more digitalized, it is also still concerned with physical aspects and human behaviour. Finally, security models often focus on a single department of interest (documentation, design of software, auditing of procedures, organisational awareness, etc.) [70].

The handful of papers of CMM related to security governance specifically does include the alignment of security policy and organisation-specific goals. A pitfall of the paper by Bruin and Solms [9] is the lack of actionable measures. This makes it hard to operationalise within the context of a specific organisation. The paper by Maleh et al. [48] is easier to operationalise and better suited for the research. The highest level of maturity (level 5 - optimized) states the following: *"Maturity reflects an information security strategy that is regularly aligned to business and IT strategies and risk appetite across the business ecosystem."* [48] (p. 228). This definition comes close to our definition of (mature) security governance, but it does not specifically mention concordance between stakeholders about this alignment. It does state that *"Information security policies and standards are periodically reviewed and revised based on input from the business ecosystem."* [48] (p. 228). If revising the security policy is concerned with the active participation and cooperation of the business, is unclear. Be this as it may, this paper is the best representation of a maturity model for security governance, that can be applied to the research and is therefore taken into consideration.

2.4. Trade-offs in security governance

Security governance was defined as the alignment between security policy and business goals, with the maturity of security governance being about reaching concordance with this alignment. Before exploring trade-offs related to security policy and business goals, it is worth mentioning that - in practice - business goals are not always aligned with the security policy, just as individual departments are not always keen on putting business interests first at the cost of their own department. To delineate further, even within departments there can be conflicting individual interests.

These conflicting interests can be troublesome for business operations. Ideally, employees work towards a common overarching business goal or objective. The 'higher' the objective, the more generic its statement becomes. Many employees perceive these overarching business objectives as vague. This often results in employees preferring more specific objectives to work towards, such as project-specific goals or interests of a department. Consequently, employees encounter trade-offs in their work.

One of the chosen dimensions of security governance is 'Direction of acquisition and commitment of resources'. Setting the direction of acquisition, making investment decisions and committing the proper resources to this (e.g. time, expertise, money, etc.), involves trade-offs. *"In government, resources are usually finite and decision makers must be aware of the trade-offs implicit in decisions they are making"* [45] (p. 4). Usually, this is a trade-off in terms of multiple risks, i.e., investing in a tool for encryption or strengthening the user awareness program. This shows why management should have a clear acquisition strategy that is aligned with organisational objectives [39].

Another interesting trade-off related to compliance in security governance is choosing between rules and principles. Gulzar and Kopcho [32] recommended this as 'just enough governance' which aims to leverage competence and context by the decision-maker instead of rigid (enforced) compliance. A rule in security governance could be: 'the security officer is responsible for internally controlling the classifying of information'. A counterpart principle for this would be: 'Everyone within the company understands the need-to-know principle and strives for the integrity of our information.' The trade-off here is that steering too much on principles alone might cause 'misinterpretation' of principles by employees. Rules are - if constructed SMART - clear and rigid. Conversely, rules can easily become outdated or too rigid. Especially for organisations operating in a fast-changing environment [32].

Yet another trade-off is knowledge sharing vs. information protection. this trade-off becomes increasingly important with the reliance on IP and better-digitalised working environments. Elliott et al. [23] describe in their paper how access to and communication of information fosters innovation and overall working productivity, but organisations are also wary of information leakage. Therefore, organisations restrict employees' access to information [23]. This could go as far as having completely separated working- and project environments, both digitalized and physical.

Apart from the trade-offs described above, there are many more trade-offs related to security governance. Even those that are not inherently concerned with governance on security can be applied to the research. Buytendijk and Willemsen [10] composed a list of ethical dilemmas within organisations. Many of these dilemmas can be projected on security governance as well. The most relevant dilemmas are described below and applied to security governance:

- **Accessibility vs. Security:** data needs to be easily accessible by employees and preferably by anyone who needs to have access. However, having information easily accessible also increases the risk of information falling into the wrong hands.
- **Security vs. Privacy:** privacy is often looked at from the perspective of a consumer. However, privacy is also relevant for company security policy. One example of this is the level of monitoring that is done on employees, both via IT systems and physically. In terms of security, more monitoring would give a better indication of the threat environment and enables tracing potential breaches in the early stages. Extensive monitoring, also impacts the privacy of employees as every (digital) step gets logged.
- **Transparency vs. Secrecy:** transparency is needed in a well-functioning organisation. In terms of security governance, employees will want to know what is going on, what to look out for, best practices and issues from earlier projects. In contrast to this, sharing everything openly might expose vulnerabilities and put the organisation at risk.
- **Getting it out vs. Getting it right:** Acquiring and rolling out solutions in a timely manner is important, but so is quality [10]. Especially in terms of the security of products and services. Insufficient (security) tested products or services can have serious consequences on an organisation. In many organisations, decisions are made that are profitable (or necessary) in the short-term. However, these decisions might have long-term risks. An example applied to security governance is the use of VTC (Virtual TeleConference) as this is easier to communicate with partners. This does bring forward an additional security risk that in the long run can be significant.

Even though the term dilemma is used, in many instances, choosing either one is not choosing out of two inherently ’bad’ alternatives. Similarly, the decision is in most cases not binary. Taking the last ’dilemma’ as an example, getting a product or service on the market fast and getting the product on the market validated/verified, is something that is usually done in tandem. However, both cannot be pursued with full commitment, as one impacts the other. Therefore, these dilemmas are better-called trade-offs. Setting a trade-off slider indicates what side of the slider one prefers to be.

If we look closer at some of the dilemmas that were described, some fundamental characteristics can be derived. Hollnagel [34] argued that these are ’Efficiency’ and ’Thoroughness’. Together these form the so-called ETTO principle: *”the fact that people (and organisations) as part of their activities frequently have to make a trade-off between the resources (primarily time and effort) they spend on preparing to do something and the resources they spend on doing it”* [34] (p.1).

The ETTO principle states how people and organisations make a choice between being effective and being thorough. It is rarely possible to maximise both at the same time [34]. However, it is possible to pursue both to a certain extent. Using the example of getting a product/service to market, the emphasis might lie on effectiveness, i.e. getting output as fast as possible. This will impact the thoroughness, as there is less time to check and test everything. This principle can be applied to other use cases as well.

3
Theoretical framework

Security governance is becoming more important as the threat landscape organisations find themselves in gets more complex. There is a need for measuring the effectiveness and maturity of this governance. The literature review of chapter 2 carefully defined the key concepts central to this study and explored the dimensions for security governance and the maturity thereof.

This chapter provides a lens for the interpretation of the research [47]. In the literature review, multiple definitions of security governance and maturity were reviewed. Based on the review, working definitions of the key concepts were drafted. This section further builds upon the definitions and perspectives from the literature review and states the assumptions, as well as orientations from which the findings will be looked at. This helps shape the lens through which the concepts of study are seen through.

3.1. Compliance versus concordance

From the literature review, it was concluded that security governance is more than just imposing a security policy on employees. Security governance is decoupled from a single department and concerns both the security policy and the business objectives. It was argued that maturity of security governance can be interpreted in different ways. The literature review concluded that both the conventional way of looking at maturity and the social view on maturity are important for a holistic view of security governance. A novel view on social maturity is the term concordance, which describes how alignment between security policies and business goals is reached. This novel view on social maturity is of key importance for the maturity framework as it parts from existing views on security governance that pursue compliance of employees rather than shaping policy in concordance with a representative stakeholder group.

Concordance originates from the Royal Pharmaceutical Society of Great Britain. It was introduced to cover the need for patients and healthcare providers to cooperate in a mutually agreed treatment programme and was the first definition to acknowledge that patients and doctors may have different views regarding treatment [67].

Prior to this, the term compliance was commonly used. Vermeire et al. [66] extracted multiple issues with the term compliance and its use in healthcare. Compliance features negative aspects inherent to the term. It suggests yielding and submission, as well as non-compliance indicating failure or the refusal to comply [66]. In the case of healthcare, compliance is the extent to which a patient's actual history of medicine administration corresponds to the prescribed regimen or the extent to which a patient's behaviour corresponds with health advice [66].

This paternalistic approach towards the patient had negative influences on the doctor-patient relationship [67, 66]. Instead, the patient should be considered as an equal and a partner, by informing and sharing decisions, as well as knowing the patient's beliefs. According to Vermeire et al. [66] *"This may lead to a negotiated treatment plan to which both patient and doctor can adhere."* (p. 340).

In the same way, the relationship between employees in an organisation can be looked at. Or, more specifically, the relationship between an employee and a security officer. Compliance, here, would be that the employee obeys all the policies, procedures and restrictions the security officer imposes on the employee. Again, this implies negative aspects like submission and yielding, as well as the lack of a mutually agreed security policy.

Concordance, on the other hand, means that both parties take on an active role in shaping the policy. It involves mutual respect and takes into account the specific knowledge, experience and perspectives of both parties [4]. This also means that 'secure behaviour' or following rules/procedures that are deemed secure, cannot be mandated by a single actor, i.e. management or the security department. Employees may have concerns about how effective certain security measures or behaviour is and how this impacts their own work-related goals and activities [59]. This might put forward implications that were not known beforehand. Apart from higher engagement from employees, thereby increasing the effectiveness of security policy, it can also lead to more efficient solutions that are better aligned with business activities.

It is worth stating at this point that the shift from compliance to concordance is relevant for this study as well. Both compliance and concordance are used in the research. In reality, it would be naive to believe that concordance in itself can completely overrule all aspects of compliance. The purpose of concordance is to include a variety of stakeholders with different viewpoints and expertise to shape policies. Eventually, however, a decision will have to be made on what this new set of policies is. This has to be acknowledged by the stakeholders involved and then executed accordingly. Even though alignment between security policies and business goals can be done in concordance, the outcomes need to be hierarchically imposed. Employees need to be compliant with this agreed-upon outcome. Within an organisation, the security department is responsible for hierarchically imposing policies and keeping oversight. This relation between compliance and concordance is something that need not be overlooked in the framework for maturity of security governance.

3.2. Misalignment and trade-offs in security governance

Another important aspect of the literature review was the definition of security governance as the alignment between security policies and organisational goals [2]. In the previous chapters, security policies and organisational goals (applied to Damen Naval) were already defined. At first sight, the term alignment might come across as straightforward. However, it can be interpreted in a number of ways. On top of that, alignment takes place on multiple levels. Alignment can be looked at from an organisation perspective, but also from an individual viewpoint. Let's first consider the basic definition and the organisational perspective.

In electronics, alignment indicates *”the proper adjustment of components of an electronic circuit, machine, etc., for coordinated functioning.”* (3) [20]. If, for example, a transistor in an electronic circuit is incorrectly positioned in relation to other components, an electronic signal might not be transmitted across the rest of the circuit, causing the machine to malfunction. Using the machine as an analogy for an organisation and components of an electronic circuit as parts of security policy and business goals, coordinated functioning is achieved if these components are adjusted properly. If not aligned, the organisation will not function properly.

Perhaps, I should also point out here that alignment doesn’t necessarily mean putting all the best components together in a machine. It entails working with what is available and adjusting components in such a way that, with the resources available, the machine works in an optimal state. In machinery, diagnostics can measure certain parameters like current drawn and temperature, but in an organisation, this is harder to do.

(Mis)alignment also occurs on the individual level within an organisation. Employees are making decisions in their work continuously, by balancing preferences and considering the consequences. Usually the decision involves a property of something diminishing in return for a gain in another property. In other words: something increases but something else must decrease. Decisions therefore can be called trade-offs. One could say that this would imply that you can never have any of the desired properties or results.

Another way of looking at this is by arguing that the trade-off is not between two desired properties, but between two extremes, e.g., having a 20-factor authentication policy and having a productivity ratio of 100% (spending all working hours on project work). It is impossible to spend all working hours on productive project work if you first need 20 different factors for logging in to your working environment, especially if this is also combined with the policy of always locking your device when you are not behind your desk.

Instead, an optimum between the two extremes can be found. Having 2-factor authentication is effective, as it lowers the wrongful login rate, but also ensures that employees can do their daily work. Arguably, this could be named a trade-off slider.

3.3. Misalignment and the effect on compliance

The hard part in setting the trade-off slider is that an individual in a company, e.g., a security officer, cannot always decide where to put this trade-off slider. If a company policy requires an employee to have 20-factor authentication, the employee cannot continue with productive work by means of 2-factor authentication. This also relates to section 3.1, as part of compliance versus concordance. If the wishes of an employee are not taken into consideration and if the trade-off slider is not set in concordance, an employee is forced to comply with (or disobey) the set policy of the organisation.

Existing literature has already put quite some effort into understanding how employees deal with potential misalignment or trade-offs between their primary tasks and security measures [7, 44, 59]. To start with, there is only so much employees within an organisation are willing to comply with. If the perceived cost for an employee to comply with security measures and policies is exceeding a certain threshold, the employee will seek ways to reduce the costs of compliance [7]. How this operationalises is very hard to predict, which makes it even more important for organisations to understand where the individual thresholds lie and how to ensure that the threshold is not exceeded. The most important way of dealing with this is by reducing the perceived costs of employees in complying, by making security measures more efficient and considering that trade-off sliders are not always skewing towards 'more security' (as it usually implies a larger cost for the employee). Exceeding the threshold does not directly result in an employee being non-compliant. For a short amount of time, the employee might still be compliant. Also, if heavy monitoring and enforcement are involved in ensuring compliance, the employee might still conform to security measures. This does, however, put a serious strain on the respective employee(s). Considering that Damen Naval is a heavily regulated organisation, this is something to take into account.

In line with the compliance budget, Kirlappos, Beautement, and Sasse [44] further investigated why non-compliance in organisations occurred. The first reason was, again, that the costs for compliance were too high. Another interesting reason was the lack of understanding of risks and/or technologies involved in security. If employees do not understand why certain measures are taken or why policies are in place (that potentially limit productivity), this contributes to employees circumventing the measures or being non-compliant completely. A final reason for non-compliance is the mere inability to comply [44]. If an organisation does not give the right resources or access for employees to comply with policies and measures. Both the willingness and the ability of employees to comply are also present in the behaviour model by Fogg [26], which states that in order for an individual to engage in target behaviour (in this case, compliance to security policies) there must be sufficient motivation and the ability to do so. The model does describe one more condition to be in place for target behaviour to occur, which is the trigger [26]. A trigger could be an announcement or reminder by the security department to do something, but it can take many forms.

Misaligned incentives, lack of understanding or the inability to adhere to security measures can all result in non-compliance. The lack of understanding and inability to comply are also a result of immature security governance. These aspects can be improved following the conventional viewpoint of maturity. The misaligned incentives, however, are a complex and wicked problem that is hard to improve upon. Especially considering that incentives are employee specific. Setting the trade-off slider for each individual employee and then converting this into security governance is not feasible for large organisations. There have been approaches to try and include the impact on employee productivity and usability of security measures, but these remain focused on specific parts of security governance. Parkin et al. [53] proposed a tool for visualising trade-offs to help security officers shape policy better related to password authentication. The tool included policy-, support- and user properties to be configured. The tool shows the number of breaches due to the authentication policy, as well as the productivity in terms of productive hours lost on authentication and the costs involved in the authentication policy [53]. Although quantification of the different parameters is difficult, the tool gives security officers and managers a more comprehensive view of what the effects are of configuring authentication policy in a certain way.

Even though the paper mentions that the tool could be repackaged beyond authentication policies, a holistic tool that can be applied to a wide range of security governance fields is not yet developed. Therefore, engaging in dialogue with representative stakeholder groups on how trade-off sliders can best be set for specific security policies, is expected to be a suitable way of reaching alignment between security policies and business goals. Concordance might not be the only goal for mature security governance, but it is an important base for this research.

4 Methodology

4.1. Research strategy

A case study was selected as the main research strategy for this research as it best suits the three conditions of Yin [71], i.e., the type of research question, the extent of control over behavioural events and the level of focus on contemporary events, for choosing a research strategy. A case study approach is a useful way of doing research for studying contemporary events in a non-contrived setting, i.e. a natural (business) environment where events proceed normally [62]. Given the topic of this research about security governance, and with that specifically the social aspects of how employees perceive working practices and security measures, a case study is applicable. The research would not benefit from a contrived setting in which all external factors are controlled. Security governance needs to be applied in a comprehensive real-world environment that is not tempered with. Only doing research in a framed environment that lacks normal organisational working conditions, will most likely not reap usable results.

On top of that, the central question of this study is a 'what' question. This study is mostly exploratory in nature, as its goal is to design a framework for measuring the maturity of security governance. Although studies have been conducted regarding security governance. No studies have investigated maturity of security governance in depth. Especially not as comprehensive as this research aims to do. Existing maturity frameworks of security governance do not include social maturity, which makes this research an exploration of what its role is within the framework. A final aspect to select a case study approach is that the data for the case study was gathered during a limited period of time, as interviews were conducted with employees and a focus group session was held. This further delineates which research strategies are applicable, as it excludes history.

4.2. Case study design

As discussed, the case for this research is the security governance of Damen Naval within the context of the naval industry. The rationale for choosing a single-case design in contrast to a multiple-case design is that the respective case is unique or extreme [71]. Damen Naval is part of Damen Shipyards Group (DSG). Globally, DSG has 12.000 employees spread over 55 companies and 35 shipyards worldwide [30]. The naval shipbuilding division of DSG is one of the few large naval shipbuilding companies in the world, which relies heavily on the protection of IP and is bound by strict regulations. The company is therefore no dime a dozen in its field and can be considered unique within the maritime industry.

To delineate the case within Damen Naval, the research was limited to the head office of Damen Naval in Flushing. Shipyards, secondary offices and cooperating companies of Damen Naval are not considered part of the unit of analysis. In order to get a holistic view of security governance within Damen Naval, no restrictions are made to departments, considering that security affects all aspects and departments of an organisation. Despite being a single-case study, the research embeds multiple units of analysis. As seen earlier, the objective of the study is to design a framework for determining the maturity of security governance at Damen Naval.

The results of the literature review formed a foundation for the initial security governance framework, by extracting which dimensions contribute to effective security governance. Based on the initial dimensions of security governance, interview questions were derived. The list was complemented by other findings of the literature review related to misalignment between security policies and business goals, as well as challenges or trade-offs that exist in organisations.

The semi-structured interviews were conducted on each individual security field with the goal of extracting performance indicators for measuring the maturity of security governance (SQ 3). Although the security fields of 'access control', 'data classification' and 'monitoring & incident control' were the focus of the research, additional findings that were not directly linked to these security fields were also taken into account. The interviews also facilitated interviewees in describing the challenges and trade-offs they endure in their daily work, to verify the trade-offs and challenges extracted from existing literature. These findings were later on used to prepare the focus group session and to set trade-off sliders, which are coupled to the final sub-question about how concordance on alignment can be reached. This final part of the research considers the maturity of security governance from a more social viewpoint, whilst the first part on security governance performance indicators is related to conventional maturity. Combined, the execution of this research design results in a framework that determines the maturity of security governance from both viewpoints into a holistic whole.

4.2.1. Unit(s) of analysis: chosen security fields

The security fields are based on components of the Damen Naval security governance model, but they are no direct copies. Instead, some fields are combined or renamed to have a clearer delineation for the research. The scope of the selected individual security fields is as follows:

Access control comprises both physical access to the office of Damen Naval and project departments inside the office, as well as access to hardware and software. Physical access control concerns access to the office and individual project floors at Damen Naval. Access to hardware like computers, smartphones and laptops is also considered part of access control. Logical access control is mostly concerned with software and the credentials needed to access computer networks, files and other data. The security field is wide-ranging on purpose as the common factors in these areas of access are authorisation and authentication of the individual.

Data classification is used to label every piece of information within Damen Naval: documents, 3D CAD models, 2D drawings, presentations, simulations and emails. For information that originates from Damen Naval, the DSNS (Damen Schelde Naval Shipbuilding) classification applies. For a project with customer security requirements, other data classifications may apply. The DSNS classifications are:

1. DSNS Public: not sensitive, anyone inside and outside of DSNS may see it;

2. DSNS Internal / commercial in confidence: can cause significant damage if falls into the wrong hands (e.g. general procedures, instructions and basic technical documents);
3. Damen Schelde Naval Shipbuilding Restricted: can cause serious damage if falls into the wrong hands (e.g. budgets, design engineering information, etc.)
4. Damen Schelde Naval Shipbuilding Confidential: very sensitive information (e.g. system passwords, encryption keys and sensitive management team information) [63].

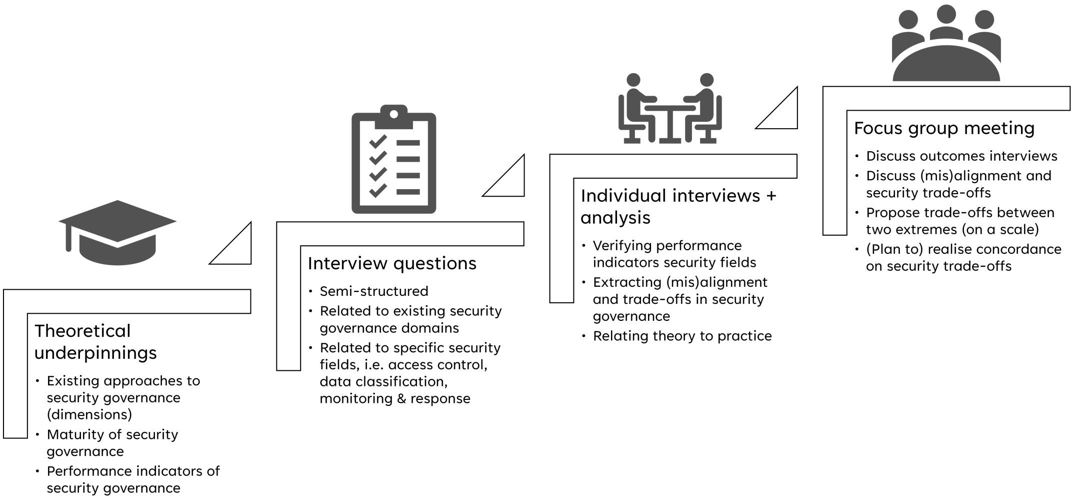
Monitoring & incident response is about surveillance of information systems, security anomalies and incidents in information systems, as well as identifying irregularities and acting upon them accordingly. Monitoring includes the logging of data by the Security Operations Center (SOC).

4.3. Data collection

Considering that a large share of the information within Damen Naval comes from employees, interviews, and observations are useful data collection methods. The methods, as well as their respective sub-questions are shown in table 4.1. To give a better understanding of the relationship between the individual subquestions, figure 4.1 displays a graphical representation of the main research components. The different data collection methods are described in more detail in the next sub-sections.

Table 4.1: Data collection for individual research questions

	Research question	**Data subject**	**Collection method**
1.	What are useful dimensions along which security governance can be assessed?	Documents	Literature review
2.	What are trade-offs related to security governance within an organisation?	Documents Employees	Literature review Interviews
3.	What are performance indicators for for security governance at Damen Naval?	Documents Employees	Literature review Interviews
4.	How can concordance be reached on trade-offs regarding security governance at Damen Naval?	Documents Employees	Literature review Interviews Focus group session



Theoretical underpinnings

- Existing approaches to security governance (dimensions)
- Maturity of security governance
- Performance indicators of security governance

Interview questions

- Semi-structured
- Related to existing security governance domains
- Related to specific security fields, i.e. access control, data classification, monitoring & response

Individual interviews + analysis

- Verifying performance indicators security fields
- Extracting (mis)alignment and trade-offs in security governance
- Relating theory to practice

Focus group meeting

- Discuss outcomes interviews
- Discuss (mis)alignment and security trade-offs
- Propose trade-offs between two extremes (on a scale)
- (Plan to) realise concordance on security trade-offs

Figure 4.1: Relationship between data collection methods and their contribution to the research questions

4.3.1. Individual interviews

Participant selection

Interviews were conducted among all levels and departments of the organisation of Damen Naval. The interviewees were selected based on their role in the unit of analysis. For access control, this included a variety of employees in different departments: security officers, the board of directors, project security, ICT and human resources. One key area where interviewees needed to be represented was in projects, which is the most critical area in terms of access control. For data classification, all different departments of Damen Naval were represented. Additional focus was placed on those employees that are responsible for classifying data and the employees that have to communicate and/or transfer classified data. For monitoring & incident response, the interviewees were similar to the other security fields, with an emphasis on the ICT and security employees. The reason why a wide selection of interviewees was chosen, was because the aim of the interviews was to gather insights from different perspectives within the company, to better understand potential misalignments in security policy and 'productive work'. An overview of the interview participants is given below:

- **Project engineer [P01, P07, P10]**
  Employees that are actively working on projects with a technical function. Participants differed in working experience and field of expertise.
- **Security officer [P02, P03]**
  Employees active in the security department, with expertise in policy-setting, security within projects and cybersecurity.
- **IT (cybersecurity) [P05, P12, P13]**
  Employees active in the IT department, with different roles and responsibilities.
- **Project (implementation) manager [P04, P06]**
  Interviewed project managers were responsible for part of a large shipbuilding project, as well as the implementation of a PLM environment.
- **Board of directors [P08, P14]**
  Representatives of the board of directors.

- **Business controller [P11]**
  The business controller was interviewed from the role within strategic acquisition of resources and financial (project) projections.
- **Human Resources [P09]**
  The department of Human Resources was represented to have a comprehensive business representation, as well as potential conflicts in access control.

Interview questions

For the individual interviews, a semi-structured approach was used. Even though a list of interview questions was prepared prior to the interviews, during the interviews there was room for exploring additional factors or conflicts that the interviewee addressed. This aims to combine the advantage of unstructured interviews, as to bringing preliminary or additional issues to the surface, with the advantage of a structured interview, to get more in-depth information about the security governance dimensions of interest [62].

The list of interview questions was applied to each individual security field. Most of the questions are overarching and applicable to multiple security fields, but some questions were security field specific. All the interviews started with introductory questions (Appendix A). The introductory questions were asked to get an understanding of the extent to which interviewees are familiar with the business goals of Damen Naval, as this is one of the two important pillars of security governance.

Next, interviewees were asked questions based on the derived security governance dimensions of section 2.2. Depending on the security field, some questions were specified to prevent too abstract answers. In general, interview questions were not altered between interviewees, with the rationale of asking the same questions to different employees, with different roles, perspectives and expertise, would result in different answers. For interviewees specialised in a certain department, e.g., finance, questions were altered to get a better sense of some of the security governance dimensions. The general list with interview questions can be seen in appendix A.

4.3.2. Focus group meeting

In addition to the semi-structured interviews, a focus group meeting was hosted to openly discuss the results of the interviews and their security-related trade-offs. The meeting had representatives from I(C)T, security and project departments (G01 - G05). Representatives were assured to speak freely and have the same amount of authority as well as input during the session. This meeting structure would facilitate potential concordance [66, 4]. The focus group was asked to discuss specific use cases for the security fields of access control and data classification. The security field of monitoring & incident response was briefly discussed, but due to the specialised nature of this security field, other respondents were not able to participate on the same level as employees working specifically on incident response.

During the discussion, trade-offs or potential misalignment between the existing security policy and the contribution to business (or project) goals were derived. Next, the representatives were asked what it would take to reach a state of alignment between these two for the respective cases and what was hindering them in order to do so. The doctor-patient relationship (as discussed in section 3.1) was used to better discuss the concepts and relate them to the focal organisation. The main goal of the meeting was to reach concordance in the alignment of business goals and security policy, thereby answering the final research question (SQ 4).

4.4. Data analysis

The conducted interviews were summarised based on audio recordings and notes taken during the interview. The summaries were written in third-person and present simple unless direct quotations were used. The interviews themselves were conducted in Dutch, but the summaries were written in English. For the translation of nouns, adjectives, imagery and proverbs that had no direct translation in Dutch, no quotes were used to prevent misinterpretation. Instead, these wordings were carefully translated to the best suitable translation, using multiple translation tools and synonyms as references. Audio recordings were played back to ensure the right connotations in the choice of words.

A multi-paragraph format was used, with each paragraph answering one question, excluding any follow-up questions. Each summary started with an interviewee introduction. The summary was written chronologically, i.e., in line with the interview and audio files. This ensured no major points were missed and made it possible to verify the summary with the audio files at a later stage. Only answers to questions asked by the interviewer and content related to these questions were included in the interview. Some participants were interviewed based on multiple security fields. For those longer interviews, the summaries were divided into multiple chapters, e.g., 'Data classification'.

The summaries were kept as extensive as possible. Merely objective statements were made, as great care was taken to not describe the interviewee's answers with personal opinions of the interviewer and exaggeration of the actual answers. In addition, quotes were added including timestamps. After summarising, additional timestamps were added to the audio files of the individual interviews. The following aspects were not included in the summaries:

- 'smalltalk' or personal information that was included in the audio file (such as questions out of personal interest in between the interview questions);
- information that could not be anonymised or generalised properly (specific company data, names and specific functions or projects);
- specific project-related information that did not (in)directly contribute to answering the interview questions;

For the analysis of the interview summaries, deductive analysis was used. The six dimensions of security governance were used to mark applicable parts of the summaries as a foundation for further analysis and to better relate potential security governance indicators. Next, a thematic analysis was performed to identify recurring themes in the interviews. One approach to thematic analysis is described by Terry et al. [64]. The paper defines a six-phase analytic process for familiarising with the data and coding (phases 1-2), developing themes (phase 3), reviewing and defining themes (phases 4-5) and, finally, presenting the final results (phase 6). The initial generation of codes was done using an inductive approach, i.e., allowing the interview data to determine the phrasing of codes. These codes were later on revised and developed. The codes were assigned directly to the audio file using labels in an offline-based audio 'viewer' (an example of this can be seen in figure 4.2. Afterwards, codes were grouped into themes and these themes were applied to the summaries of the interviews and related to the initial security governance dimensions. This led to additional themes in section 2.2. The topics 'Virtual Video Teleconference (VTC)', as well as 'Screening implications on the workforce' were derived from this thematic analysis but were later coupled to the security governance dimensions. The results of both the deductive and the thematic analysis laid the foundation for drafting the performance indicators.

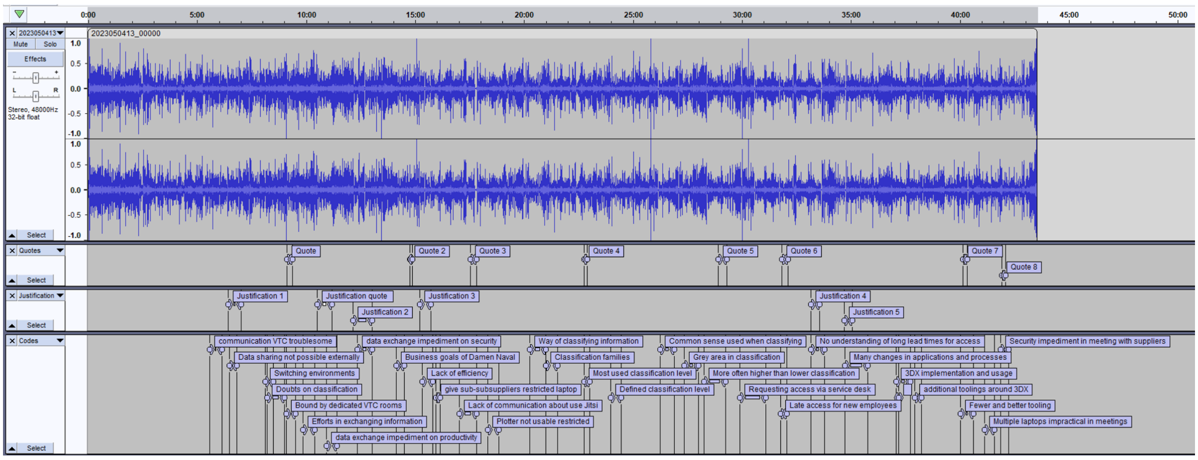

0:00
5:00
10:00
15:00
20:00
25:00
30:00
35:00
40:00
45:00
50:00
2023050413
Mute
Solo
Effects
Stereo, 48000Hz
32-bit float
2023050413_00000
1.0
0.5
0.0
-0.5
-1.0
Select
Quotes
Justification
Codes
Quote
Quote 2
Quote 3
Quote 4
Quote 5
Quote 6
Quote 7
Quote 8
Justification 1
Justification quote
Justification 2
Justification 3
Justification 4
Justification 5
communication VTC troublesome
Data sharing not possible externally
Switching environments
Doubts on classification
Bound by dedicated VTC rooms
Efforts in exchanging information
data exchange impediment on productivity
data exchange impediment on security
Business goals of Damen Naval
Lack of efficiency
give sub-subsuppliers restricted laptop
Lack of communication about use Jitsi
Plotter not usable restricted
Way of classifying information
Classification families
Most used classification level
Defined classification level
Common sense used when classifying
Grey area in classification
More often higher than lower classification
Requesting access via service desk
Late access for new employees
No understanding of long lead times for access
Many changes in applications and processes
3DX implementation and usage
additional toolings around 3DX
Fewer and better tooling
Multiple laptops impractical in meetings
Security impediment in meeting with suppliers

Figure 4.2: Example of codes in audio file interview

4.5. Quality assurance

In order to improve the validity of the overall research, triangulation is used. The basic idea behind this technique is that using more sources or methods will lead to a more confident research outcome [62]. Triangulation can be practised from multiple perspectives. The most common are method, data and theory.

Triangulation of method is realised by implementing multiple forms of data collection and analysis. For this research the data collection methods include literature research (desk research), individual interviews and a focus group meeting. Data triangulation occurs when data is collected from different sources and at different points in time. This is done by interviewing different employees from different departments. Apart from triangulation, the quality of empirical exploratory research is commonly established by three different tests:

1. **Construct validity**: identifying how well the results from the use of operational measures fit the theories around the design of the test [62].
2. **External validity**: the extent to which a study's findings can be generalised [71].
3. **Reliability**: demonstrating that repeatability of the research is possible and will result in the same results [71].

Construct validity is one of the more challenging tests for case studies as it is difficult to develop operational measures free from subjective judgements [71]. For this research, the construct of 'maturity of security' or 'security maturity indicators' is hard to operationalise. Especially since the research itself aims to generate generalisable maturity indicators. Nonetheless, carefully defining the constructs will at least demarcate what is meant by the constructs and will keep interpretation to a minimum. On top of that, the research design implements three units of analysis; 'access control', 'data classification' and 'monitoring & incident response. These units of analysis are studied to a more detailed level, thereby making it easier to operationalise the measures and being able to compare this with the literature about the measures.

External validity overall is hard to achieve when choosing a single case study design [71]. To improve the ability to generalise the research, the research design incorporates multiple units of analysis. Even though the research is based on a single case, it has multiple sub-cases embedded. As the purpose of this study is to come up with a framework for determining the maturity of security governance, the external validity benefits from this aim.

Reliability of the research is achieved by implementing a case study protocol so that the research is repeatable by someone that was not involved in the initial research. The goal is to minimise biases and errors during the research. Another way of ensuring the reliability of the research is to carefully collect and process data. One could argue that not transcribing interviews impacts the reliability of the research, as summaries tend to be more selective and interpretive [33].

The rationale behind summarising the individual interviews instead of verbatim transcription consists of multiple elements. First, thematic analysis does not specifically require a high degree of closeness to the data [33]. At least, not to the extent that transcription is done word for word, or includes stuttering and silences. Also, the interviews were conducted in the native language of the participants, i.e., in Dutch. This would make word-for-word transcription impossible, as a translation would have been necessary at one point. The interviews were conducted in Dutch on purpose as interviewees in principle feel more comfortable expressing themselves in their native language and being less impacted by potentially limited vocabulary. Even though this might negatively impact the data analysis to some extent, as the interview audio had to be translated, it was expected to make up for this in the richness of the answers of the participants.

Second, the summaries of the interviews were shared with the respective participant afterwards. Respondents then had to verify if the interview summary was valid or if changes had to be made. Misinterpretations or wrongful phrasing could thus be filtered out. Changes were only made if something was not aligned properly with the audio recording.

Third, great care was put to ensure that comprehensive and systematically composed summaries were made. The summaries were drafted as objective as possible with minimal bias and interpretation of the actual audio files. The procedure of how the summaries were derived is described in section 4.1.

Fourth, the context of the research and the case study at Damen Naval contributed to choosing summaries over verbatim transcription. Due to the topic of security and the business environment of Damen Naval, with heavy regulations regarding confidentiality, summaries were a better fit for this research. A security officer of Damen Naval had to review the summaries of the interviews, after being approved by the interviewees themselves, to ensure that no harmful information to Damen Naval was used in the writing of this thesis. Changes that had to be made regarding the interview summaries were indicated in the respective summaries, to indicate that there was a discrepancy with the original document.

Fifth and finally, the interviews were analysed both inductively and deductively. A deductive analysis is less bound by semantic meaning in the data of the interview. Therefore, this is better suited to apply to summaries. For the interview, an inductive approach was also chosen, but the first-level coding was done directly in the audio file of the interviews, which enables analysis directly on the raw data.

4.6. Ethical governance, confidentiality and data management

This research has been approved by the Human Research and Ethics Committee (HREC) of the TU Delft. In line with the context of the research, additional thought has been given to safeguarding data as well as confidentiality. An extensive data management plan has been drafted and discussed with a data management steward at the TU Delft. The complete HRE application has also been reviewed by the advisory team knowledge security. Audio recordings of the interviews were stored on a local audio recorder and kept on-premise. Having done these additional measures, the HRE application was approved.

5
Results

In attempts at understanding and measuring the maturity of security governance, extant literature has primarily focused on the security policy itself and its technical implications within organisations. There is, however, another important aspect to consider, which is the extent to which the security policy of an organisation is aligned with ’the business’. By analysing useful dimensions along which security governance can be assessed and by exploring trade-offs or fields of (mis)alignments between security policies and business activities, a novel way of looking at security governance can be derived.

This chapter reports on the findings from the analysis of the conducted interviews. The interviews were analysed based on the chosen dimensions of security governance from section 2.2 and are described further in table 5.1. The interview findings show how the security governance dimensions are operationalised within Damen Naval and indicate the performance on these dimensions. For each security governance dimension additional themes from either the inductive or deductive analysis were coupled. Based on the security governance dimensions and the interview results, specific performance indicators were derived that help determine the conventional maturity of security governance. Finally, representatives of different departments at Damen Naval were invited to further discuss the analysis of the individual interviews, by discussing a number of specific cases related to the security fields and the inherent trade-offs or challenges that were perceived. This final part focuses on the social maturity side of the framework by exploring how concordance can be reached in the alignment between business goals and security policies.

Table 5.1: Security governance dimensions used to analyse interview findings

Dimension	Description
Organisation-wide security and responsibility/accountability	Interview findings related to individual or shared responsibility/accountability for security or the consequences of security. Also includes the process of decision-making for security-related issues.
Risk-based approach	Interview findings that are concerned with the risk appetite of the organisation, the extent to which security measures need to be taken based on the threat landscape and other (in)direct consequences
Direction of acquisition and commitment of resources	Interview findings about the extent to which the impact of security (measures) is taken into consideration when acquiring new resources, such as software platforms, working environments, etc., as well as (the lack) of commitment from management to acquire certain resources.
Conformance with internal and external requirements	Interview findings related to (the lack of) conformance to internal requirements, such as the security policy and derived protocols, as well as external requirements, such as those from clients or international regulations.
Security positive/conscious culture	Interview findings about how employees perceive security within the organisation, their security awareness and engagement.
Security performance measurement/ alignment	Interview findings about the performance measurement of security measures and the extent to which they are fit for purpose, i.e., applicable and effective to use in the current and future working environment of the organisation/industry.

5.1. Security governance dimensions operationalised

5.1.1. Organisation-wide security and responsibility/accountability

Shared responsibility or lack of ownership?

A respondent said that everyone should know who the owner of information is to authorize access (P03). However, when asked to describe the chain of actors in the process of access control, interviewees were unsure if - currently - there is an owner of this process and related information (P06). One of the respondents mentioned that the PSO should be involved in auditing if privileges and access rights are in order, but (project)managers should be accountable for authorisation (P06).

This strive for ownership also extends to data classification. One interviewee expected that a person who approves a document, i.e., a senior engineer or project manager, is owner of the document. However, the current official policy of Damen Naval is that someone who creates the information, classifies the information, and with that, is the owner of the information. A rationale behind the latter is that someone who creates the information, usually an engineer, has the most technical expertise and know-how to understand what the implications of the data are. Engineers are thus better suited to determine what information should have what (type of) classification, according to an interviewee (P08). Generally speaking, this opinion was shared across the respondents, but some engineers were still hesitant in their ability to always 'correctly' classify information, as one engineer mentioned: *"I can only assess this [to classify data] based on my paradigm of shipbuilding and this doesn't mean that it is the right conclusion."* (P01, recording 00:47:40).

The discussion about responsibility and accountability can also be addressed from the perspective of monitoring & incident response. One ICT cybersecurity employee argued that, with incident response, the wishes and requirements of the business have to be taken into account. More emphasis should lie on conducting business impact analyses and understanding what the confidentiality, integrity and availability of certain systems are. He would go as far as saying that: *"The business determines the value of systems. This is not my responsibility."* (P13, recording 00:08:58). The interviewee believed that: *"If they determine the value on a* *good, efficient and mature manner, this will help me tremendously in incident response cases."* (Recording, 00:09:03). This would indicate that the valuation of business assets is the responsibility of the business, whilst the protection of these assets is the responsibility of ICT security.

At Damen Naval, multiple departments are concerned with security in their primary working activities. ICT security is part of the ICT department, but is tasked with the execution of monitoring & incident response, as well as ICT security measures. Next to this, there is the security department. This department sets the security policy and oversees compliance with this policy. Within the security department, there is a cybersecurity officer and there are multiple security officers working on projects. Interviewees found it hard to understand the differences and task descriptions between these departments (P09, P13). One ICT employee stated: *"Where ends the role setting and naming of the security authority and where does mine start?"* (P13, Recording, 00:35:42).

Within the security department, a project security officer mentioned that his role in the drafting of policy documents inherently brought forward some form of responsibility and accountability over the policy (P03). Even though this, in principle, was not part of his individual function, as this is something that should be carried by the whole security department. He stressed that responsibilities for tasks should be clear within the [security] department, as *"if everyone is responsible, nobody is."* (P03, recording, 00:50:10). Having a clearer framing of roles and better organisation for the security department would, according to the interviewee, promote the governance of security and positively impact the business.

Communication between departments

A recurring finding of the interviews concerns itself with communication between departments, or the lack thereof. One of the interviewees mentioned: *"There is a wall between security, ICT and the project."* (P01, recording 00:29:10), indicating that better communication is needed to understand the needs of the project, as well as the limitations and/or implications of ICT and security (requirements). Organisation-wide security is also related to expectation management, as one interviewee pointed out that he does not have the time to email security about proposals for implementation of certain IT-solutions, considering that 'the business' needs to reach deadlines and wants a speedy implementation of software (P04). According to the interviewee, organisation-wide security should be implemented as a circular process, instead of a one-way street, wherein departments actively engage and put forward expectations on security and their implications on productive work (P04).

Overall, the respondents agreed that data exchange across projects and between environments (restricted and standard) is necessary for a secure functioning business (P01).

5.1.2. Risk-based approach

Defining the threat landscape

The first aspect to point out relating to a risk-based approach is the threat landscape Damen Naval is operating within. Overall, the respondents described the threat landscape in line with the security policy of Damen Naval (P02, P05, P08, P11, P13, P14). Respondents could describe this threat landscape in great detail and also how the 'attractiveness of data to enemies' (P01) influences the security policy of Damen Naval. The war between Ukraine and Russia, as well as the relationship between Taiwan and China, shape a specific threat landscape (P08). One respondent working on incident response (P05) argued that ransomware organisations are the most profound threat actors. Followed by hacktivism and activism parties, as well as espionage, state-sponsored or private. Espionage is considered to be a more static threat (P05). Another respondent added that espionage across the internet is done by almost every (state) actor out there (P08) and that people are becoming more aware of these expectations towards espionage, resulting in more careful behaviour. Ransomware activities are more dynamic as actors, goals and methods are constantly changing (P05). One respondent argued that the threat landscape is changing as "The enemy never sleeps" (P02, Recording 00:08:38), with an emphasis on phishing (P02). Another interviewee mentioned that due to the dynamic nature of the threat environment, it is hard to continuously improve processes and procedures (P05). The interviewee believed that parting from procedures in case of emergencies should always be allowed: *"Would you rather ensure the continuity of your organisation or adhere to procedures?"* (P05, Recording, 00:16:43).

Risk Appetite and risk acceptance

The next theme where multiple codes were grouped, which corresponds to a risk-based approach, is the actual risk appetite of Damen Naval. Risk appetite and risk acceptance relate to different other themes of security governance but are covered individually to understand the different aspects involved with it. First, classification of data is involved with risk appetite and acceptance. Classification is mostly bound by internal or external requirements, but upon deviation, risk appetite and risk acceptance get involved. Respondents were asked about the consequences of classifying information higher and lower. Classifying too low, can, according to one of the interviewees, result in a data breach or unauthorised access (P03).

Classifying too high is no direct issue for security, but impacts practicality as well as costing the organisation time and resources (P03, P10). These resources are, more often than not, unavailable, which may lead to risk acceptance. One interviewee gave an example where information with a certain classification needed to be shared with an external party. Common practice was to reproduce the whole information set to something with a lower classification that is shareable, but this would lead to more time and resources being consumed. *"What is more effort? Asking the project to borrow an engineer for 14 days to convert a whole subsystem into something else [that is shareable] or find another solution?"* (P12, Recording, 00:22:29). The interviewee mentioned that this other solution was to exchange the information, but with acceptance of the additional risk.

Interestingly, the interpretations of the risk appetite, and especially, who defines this appetite and bears potential consequences, differed among interviewees. An employee of the security department responded: *"The business is the one who takes risks and we are there to support the business."* (P03, recording, 00:12:20). This utilizes an advisory role on what consequences a certain risk appetite might have on the business. However, outside of the security department, this belief was not supported by every respondent, as one employee argued that the security department is responsible for the risk acceptance and for the decision if something is allowed. *"It comes down to if something is allowed, it is impossible to have 'x' determine that it may or may not. This should be someone within the appropriate role within Damen. In this case, the security officer."* (P12, Recording, 00:25:02).

5.1.3. Direction of acquisition and commitment of resources

Implementation of a new Product Lifecycle Management platform

Damen Naval has acquired and implemented a new Product Lifecycle Management (PLM) platform, 3DX, for the execution of new projects. An implementation manager for this PLM platform argued that a PLM implementation is one of the most costly implementations an organisation can indulge in (P04). *"An SAP implementation, in terms of budget, costs 10 times less than 3DX [PLM].* (P04, Recording, 00:07:02). An SAP implementation, which is a form of Enterprise Resource Planning (ERP) is already a very large and expensive implementation on its own.

Damen Naval cannot prove or guarantee when this implementation has a return on investment, as it lacks control over data and KPIs. The high interpretability of these goals makes them harder to prove as well (P04). Also, the security policy affects the core business of Damen Naval, including the implementation of PLM (P04). *"Is it 20, 30, 40%? We don't know because we do not monitor and oversee this in a SMART manner."* (P04, recording, 00:14:55).

In addition, the interviewee believes that there is a lack of support by security for software implementation. *"What do these side effects cost? What does this mean for the business and is this worthwhile?"* (P04, recording, 00:15:55). Apart from the additional costs, the implementation of 3DX has not succeeded completely in replacing other tools for working on projects. One interviewee mentioned that: *"People say that 3DX is the single source of truth. On the other hand, there are numerous tools that work around this."* (P04, Recording, 00:40:08). Employees would prefer to have fewer tools that are more comprehensive (P10, P07).

Split environments, double the costs?

In the same way that employees would prefer fewer tools, the vast majority of the interviewees also mentioned that maintaining two individual working environments, restricted and standard, causes additional costs and issues with productivity (P01, P03, P04, P07, P08, P09, P10, P13, P14).

In terms of costs, one interviewee mentioned the following: *"License costs are doubled because every program is hosted in both environments separately. The IT landscape is doubled which also means two times the costs."* (P08, Recording, 00:18:20).

In terms of productivity, interviewees feel impacted by the double environments, as communication is difficult and applications are slow (P08, P10). *"If you want to call someone or show something, currently this is not possible, so then you will send an encrypted email."* (P10, Recording, 00:09:08). The interviewee even stated that: *"Security makes it difficult to have meetings with the supplier."* (Recording, 00:41:56). On top of that, working with two environments puts a strain on employees, as they need to maintain both environments, e.g., mailboxes, instead of one (P01).

The interviewee also believed that this might have a negative effect on security itself as more steps are required to share information with suppliers and a mistake can be made more easily (P01). Another interviewee stated that separate environments and applications for each project would only hinder *"the good path"* (P13, Recording, 00:25:00), explaining that everyone with malicious intentions will still be able to transfer data outside of the [secured] environment.

One respondent mentioned that the most important part of functioning projects is *"being able to work together with internal and external stakeholders, and relying fully on the exchange of information."* (P13, Recording, 00:27:16). However, according to the interviewee, the opposite is currently the case, as the model that is now used is a "*castle where we put information in, with the purpose of as less as possible communication with the outside world.. So, "inherently, this does not match with the business philosophy."* (P13, Recording, 00:27:34).

Another respondent argued that having two distinct environments does not necessarily have to be significantly costly to productivity, stating that: *"This depends on how the environment is arranged."* (P11, recording, 00:20:25). If the environments allow for easy switching via software and hardware, the respondent does not believe that employees perceive this as a big issue. However, the employee also mentioned that: *"The moment you make it cumbersome to implement security measures, there is a higher chance that people will not comply."* (P11, Recording, 00:21:30).

The split environments and the inefficiency can also be considered from a commercial perspective. A business controller at Damen Naval talked about the additional hours the security measures took and how this was seen commercially. *"I have to count 2 hours instead of 1 hour for drafting a document. But if I count 2 hours, my project will become so expensive that the client would not agree. So let's see what we can do to reduce the time to 1,5 hours."* (P11, Recording, 00:11:25). The interviewee stated that this would mean investing a little more and not charging everything back to the client. According to the respondent, this is a balancing act in terms of what Damen has to absorb and what can be charged back. When asked who would absorb this additional cost in the organisation, the interviewee mentioned the following: *"We know from practice that it will take around 2 hours to complete, but you receive 1,5 hours of budget and that is what we are aiming for."* (P11, Recording, 00:13:00). Even though P11 did elaborate that there should be ways to do things in a more efficient manner, he also argued that Damen Naval should not become an officeholder culture, in which everything takes as much time as needed.

Although, overall, respondents were not fond of the split environments due to higher costs, impact on productive work and consumption of resources, one respondent mentioned that the standard and restricted environments are already better than they were (P09), with functionalities within the restricted environment working better than they used to be.

Virtual Video Teleconference (VTC)

One of the subsets of the split environment, which requires additional attention due to the issues with both security and productivity, is the use of Virtual Video Teleconference (VTC) tools. MS Teams is a tool that may be used in the standard environment for lower classification levels. For higher classification levels in the restricted environment, another VTC-tool is used. Interviewees mentioned that having to use these tools simultaneously is impacting productivity (P07, P10). P07 even mentioned that *"People get frustrated with too many different tools and solutions."* (P07, Recording, 00:21:40). P10 stated that Teams was not available via a portal on the restricted environment, which resulted in the interviewee having to use two laptops at the same time or book an additional VTC meeting room to host Teams (P10). *"If you want to call someone or show something, currently this is not possible, so then you will send an encrypted email."* (P10, Recording, 00:09:08). The respondent was therefore bound by other tools like email for communication. Quickly and easily communicating with suppliers was drastically impeded by these security measures, as *"Security makes it difficult to have* *meetings with the supplier."* (P10, Recording, 00:41:56). This other way of communicating arguably also has a negative effect on security, as the interviewee has to execute more steps to communicate and might make a mistake more easily (P10, Justification recording, 00:12:09).

Management commitment

Relating to management commitment, Damen Naval has structured the security department to be answering directly to the board of directors ([63], P02). A representative of the board of directors mentioned that employees working on large projects are working under quite a lot of pressure, with the biggest factor being the increased security restrictions on the new projects imposed by the client (P14). "People perceive that they cannot achieve the productivity that they would want to achieve, that they are being held back and that the IT environment is not in control." (P14, Recording, 00:07:27). Management is aware of these issues and aims to relieve the pressure as much as possible (P14.). In line with the commitment of resources, interviewees were asked if the higher costs of projects due to security measures, are taken into consideration with expectations for future projects. One of the management representatives stated that: *"It is very difficult to prove that the budgets are sufficient if it is unsure what the actual costs are."* (P14, Recording, 00:25:02).

Business growth and its implications on available resources

"Our IT department has grown from 25 people to 140 people in 3 years' time." (Recording, 00:10:54)." "At the same time, we currently execute 77 projects, with 60 more projects in the backlog. Of these 77 projects, a few are the size of 'implement 3DX' [large engineering package] and 'implement SAP [large ERP package]." (Recording, 00:11:02). These projects have to be executed by 15 project leaders and 9 engineers, which puts too much pressure on the department to implement and realise everything. (Justification, recording 00:11:14). Also, the interviewee believes that an implicit choice has been made to manage the IT department project-based. There is no overarching landscape or overview, and neither is there sufficient portfolio management. According to the interviewee, this was troublesome and caused ad-hoc requests. *"Everyone from the business just walked in at IT got a seat and told them they needed something."* (Recording, 00:12:52). Starting with portfolio management will ensure that there is a business owner who organises and sponsors the project.

5.1.4. Conformance with internal and external requirements

Many research findings were grouped based on the security dimension of conformance to requirements. These requirements were taken both from the internal policy of Damen Naval, as well as any external requirements Damen Naval needs to adhere to. Before addressing individual themes/aspects that were derived from the interview analysis, it is worthwhile to present some overarching findings relating to the conformance to internal and external requirements, or the lack thereof.

The majority of the respondents that were asked about adherence to regulations mentioned that Damen Naval has to conform to any external requirements imposed on the organisation or on a project (P01, P03, P07, P08, P09, P10, P11, P12). Opinions differed between the respondents as to how regulations should be interpreted. Some respondents argued that the external requirements directly translate to an internal policy for Damen Naval (P07, P08). *"Eventually, we want to be compliant with our customer requirements. This is derived from the overarching business goals of Damen Naval. If this means that we have to comply with a certain ABDO level, this then leads to a certain policy for access to certain projects or information."* (P08, Recording, 00:12:48). Conforming to requirements was also seen as a necessity for making ships (P03, P10). *"If you want to make a successful product, you have to adhere to these regulations."* (P10, Recording, 00:14:50). One interviewee did mention that: *"Secure is secure, but you need common sense to deal with it."* (Recording, 00:01:50). Another interviewee supported this by stating: *"The company policy is there to adhere to client requirements, but not more than what is required."* (Recording, 00:08:20).

Another respondent considered more flexibility and interpretability in terms of how to conform to these regulations. *"I think we look at the ABDO too soon, instead of at the business. Even though the business should conform to the ABDO, there is flexibility in the way this is done."* (P03, recording, 00:11:56), followed by: *"There is no discussion that we need to conform to the ABDO. However, the way we conform to the ABDO is open to interpretation and can be better suited to the business."* (P03, recording, 00:14:20).

A few interviewees acknowledged that even though regulations need to be followed, it would be fruitful to discuss what potential changes can be adopted in the (near) future (P08, P13, P14). The main arguments for engaging in dialogue with clients are that some of the restrictions by the client hinder productivity but are arguably also less secure than other more modern solutions (P08, P09, P13, P14). One of the specific recurring issues with external regulations (Dutch ABDO) is that cloud solutions are prohibited for project-related information. One of the interviews described how this is currently dealt with: *"There are certain Microsoft licenses, that are very secure [according to specialists], but cloud-based. So, we cannot use those [due to regulations]. What we try to do here, is imitate what these licenses can do, but then on-premise and with a marginal budget compared to what Microsoft has."* (P14, Recording, 00:25:55). Another interviewee agreed but also explained why deviation from this requirement is currently not possible: *"A lot of large organisations say that the cloud can better be secured than a single private network. However, we have to be compliant and therefore we cannot make that decision. Because it is a strict regulation."* (P08, Recording, 00:14:30).

Due to this, respondents indicated that it would be best to get in contact with the client and discuss if their regulations are still relevant and if something can be changed in the future. This would then contribute to a more efficient/secure solution for Damen Naval (P08, P13). Another respondent pointed out that recently an industry-wide lobbying group was formed that is related to the ABDO in one way or another (P14). This lobbying group has an interest in different regulations (e.g. the use of cloud services) and tries to convince the client to allow working in another way that is more beneficial for both security and efficiency (P14).

Finally, one interviewee mentioned that even though external regulations impose security measures and ways of working on Damen Naval, this should not be implemented as a strategy of the security department of Damen Naval. One of the critiques that was given to the security department and its internal security policy, was that it lacks a clear vision and strategy. The interviewee suggests writing a position paper, in which Damen Naval is proactive in its strategy and goals, instead of following what external regulators impose on the industry (P13). This would entail that even though the regulations are what they are, Damen Naval is aiming for an ideal situation that encompasses 'x' rather than 'y'.

Classification: 'Black and white' or grey?

During the interviews, a lot was said about data classification. People had different views on what should be classified, how it should be classified and also how to interpret the classification levels. The procedure for classifying information itself is clear to most employees (P07). However, respondents argued that the different classification families are confusing (P07, P13). One interviewee proposed a different way of describing what the different Damen Naval classifications mean:

- Damen Naval internal: “classification that can be chosen if everyone within Damen Naval may see this information.” (P13, Recording, 00:21:08)
- DSNS restricted: “information that should only be accessible by your own department.” (P13, Recording, 00:21:14)
- DSNS confidential: “information that is so special that only part of a department may access this information.” (P13, Recording, 00:21:22)

The majority of the interviewees that were asked about how data is commonly classified within Damen Naval, responded that they believe information is classified higher more often than lower (P01, P03, P 10). *“Data is classified too high more often than too low.”* (P01, recording 00:39:35). Another interviewee mentioned that if employees are unsure about a level of classification, they discuss this with the security department and other colleagues or *“..will take the highest level [classification] because then I’m safe.”* (P03, recording, 00:36:18). P07 also mentioned that employees are sometimes ’rather safe than sorry’ and classify information as restricted in cases where this might not necessarily be needed. He also mentioned that overall, information is classified correctly, especially if there are no negative consequences to classifying information (P07).

If there are consequences to classifying information, employees tend to act differently. P03 mentioned that in some situations, an employee is unsure if the information is restricted or confidential. In that case, he will try to classify information as restricted rather than confidential, as confidential information imposes more limits on productive work (due to the fact that this information cannot be accessed from the restricted environment). Classifying too high could, according to one interviewee, result in unnecessary taking measures such as encrypting (P07). This is supported by P03 who stated that classifying too high impacts practicality as well as costing the organisation time and resources.

The discussion of classifying information as too high or too low, was accompanied by the discussion of what would be a correct classification in the first place, as one interviewee stated that “Guidelines of classification are a grey area” (P01, recording 00:40:18). The interviewee mentioned that depending on the (technical) knowledge and view of the assessor, classifications can differ. *“I don’t have the knowledge of all facets to decide if something is restricted. I wouldn’t be able to build a ship with the information, but even if something does not seem restricted to me it might be to someone else who has more technical expertise on the matter.”* (P01, recording 00:44:40).

Another respondent argued that *“95% of the ship does not have to be secure.”* (P04, recording 00:41:30), claiming that a lot of information is not restricted and can, in principle, be accessed from a standard environment as many individual parts from the ship can be bought in a regular store (P04). The interviewee did mention that some assemblies and locations inside the ship may be restricted, as well as the weapon and radar systems (P04). Another interviewee mentioned that even complete weapon systems may be handled without additional security measures or data classification, depending on the project and client (P08). An interviewee believed that too much information was now unnecessarily in the restricted environment for the project. *“Everything is in restricted and therefore NfD [higher classification]. But not everything is NfD; the majority isn’t.”* (P04, recording, 00:44:55). This was supported by another interviewee who described the following: *"If you look at a frigate, what is truly confidential? How far it can shoot, when it is visible, radar signatures, noise, etc., but the anchor? This is not confidential. A lot of information can be handled on quite a low classification."* (P08, Recording, 00:02:54). The interviewee, therefore, agrees with other respondents that classifying information is a grey area.

Respondents were also asked on what grounds they classify information. One interviewee mentioned that he used a PDAL (Product Drawings and Associated Lists), where classifications were set by the client of the project (P10). Another respondent also believed that the client should classify information: *"We are not the ones who need to classify information. The client should do that, as they classify a project according to a certain reasoning."* (P08, Recording, 00:39:00). P07 also argued that Damen should conform to the classification requirements of the client. Another interviewee mentioned that drafting of classification levels should be aligned with project goals, as, according to the interviewee, the whole idea of data classification is ensuring that enough (but not too much) is done on security. *"The alternative would be to classify everything on the highest level."* (P03, recording, 00:34:14). Alternatively, information is classified according to common sense (P10), but also from expertise of engineers (P08, P12) and internally drafted guidelines (P07).

Need-to-be and need-to-know: define 'need'

Not only data classification was considered to be a grey area. Different interviewees brought up the principles of 'need-to-be' and 'need-to-know'. These principles are part of the security policy for access control at Damen Naval and define that employees may only have access to physical locations (to be) and information (to know) if this is required by their specific role or function (the need). One employee mentioned that: *"Need-to-know sounds very black and white, but in reality it is a grey area. Because when do you have the need to know something or to get somewhere?."* (P03, recording, 00:29:45). To give an example, the same interviewee described a situation with a line manager who does not require access to a certain project department given his role. However: *"A line manager has the need to talk to his people and therefore a reason to be somewhere."* (P03, recording, 00:29:54). The same interviewee understood that there are also implications in interpreting the principles differently. *"The question is if this is the right consideration, as the more people have access to something, the higher the chance of something going wrong."* (P03, recording, 00:30:05).

Another interviewee argued that employees working on the same project would have to have access to each others' work in order to learn from each other and align their own work with colleagues. This would be beneficial for the (technical) design. Therefore, the interviewee would prefer a different vision regarding this principle (P07). He would go as far as saying that confidential information should also be accessible to everyone working on the project. As of now, a different laptop is required to access this information. Even though most employees working on a project have the right screening to potentially access this confidential information, they are unaware of the information and/or the process of accessing the information via the confidential laptop (P07). *"People do not know how to access the information or where to find it. Because they do not know how it works; it seems like a lot of effort so they don't bother doing it."* (P07, Recording, 00:18:17)

Other interviewees had fewer issues with the principles of need-to-know and need-to-be. One interviewee argued that dealing with this policy is within the ability of individuals to find a practical solution (P11). He proposed multiple solutions for staying in touch with colleagues, even though access to certain departments was not granted due to the need-to-be principle. The interviewee also perceives the impediments that some employees have to be feelings rather than actual unfixable problems, in some situations. *"I think it is more of a feeling that they feel restrained, while in fact, this isn't really the case."* (P11, Recording, 00:37:59).

Screening implications on the workforce

One of the external requirements from clients is that the workforce of Damen Naval needs to have a certain screening. Screening by the Dutch Military Intelligence and Security Service (Dutch: Militaire Inlichtingen- en Veiligheidsdienst, MIVD) is necessary to be able to work on certain projects within Damen Naval. In principle, only NATO-countries can receive a 'certificate of no objection' (Dutch: 'verklaring van geen bezwaar' VGB). According to one interviewee this considerably limits the pool of potential employees. *"For some vacancies, we get a faster response by people from India or Pakistan compared to the Netherlands. In contrary to other divisions of the [Damen] group, we cannot make use of those people. This has nothing to do with discrimination.., ..but these people can simply not work here, because they will not pass the screening."* (P09, Recording, 00:10:58). *"If you originate from the middle east or South America and you do not have a double passport, so at least the Dutch nationality, then it ends there."* (P09, Recording, 00:09:55). Regarding human capital, the business goals of Damen Naval, therefore, do not align perfectly with the security policy, as it limits whom Damen Naval can attract to the workforce (P09).

5.1.5. Security positive/conscious culture

Understanding of security-critical endeavours and awareness

Most participants were able to describe the threat landscape of Damen Naval in detail (see subsection 5.1.2. P01 mentions that due to the threat landscape, Damen Naval cannot be too careful in its security policy even though it is considered to be significantly challenging in productive work. This is in line with P04 who believes that security belongs to the products that Damen Naval produces. The respondent argues that this is easily matched with the naval and combat aspects of the company. Employees, therefore, understand that security is part of operations at Damen Naval, which also gives people more patience (P04). One example of an interviewee who understands the necessity of security is given by P01, who responded on an issue related to knowledge-sharing: *"It's simply not possible: I cannot make a print screen of a cooling water system in restricted and pan this out in a use-case for the standard environment."* (P01, recording 00:23:30), acknowledging that even though anonymising or rewriting best practices takes more time and effort, it is necessary for a secured functioning business. Even though most interviewees are aware of the threats imposed on the organisation, the understanding of and potential consequences of ICT tools are not clear to every employee. *"We have employed a lot of smart people, but IT is getting quite complex and not everyone can comprehend when something is safe within the IT environment and when not."* (P08, Recording 00:37:51). Relating this to the papers by Kirlappos, Beautement, and Sasse [44] and Fogg [26], some employees lack the ability to engage in target behaviour, which might lead to non-compliance. A side-note here is that the ability is not related to security per se, but rather the technologies that employees work with.

In line with this, the lack of understanding of IT solutions contributes to a perceived burden being imposed on employees (P04, P08), as well as frustrations due to longer approval times for IT security-critical endeavours (P01, P07). *"To me, this is very frustrating, annoying and obstructive."* (P07, Recording, 00:31:58). P14 explained that, until recently, the relationship between IT and the business was not very good. With new IT management, *“there seems to be more understanding for IT by the business, but still, it is quite premature”* (P14, Recording, 00:35:30). Apart from the lack of IT understanding, P11 gave an alternative explanation for the perceived impediments of employees. He argued that these feelings are related to the type of projects and the considerable growth the organisation underwent in the last few years. *There are people who have witnessed the ‘old’ organisation, where you could just walk in everywhere and get a cup of coffee with colleagues. This is not possible anymore.”* (P11, Recording, 00:38:25). According to the interviewee, the organisation and the culture changed with the growth of the organisation (P11). P09 argued that the security impediments should be considered in an alternative way: *“Security should be seen less as an impediment and more from the perspective that it is part of the [new] working activities.”* (P09, Recording, 00:33:18). The interviewee also argued that Damen Naval should do more regarding security awareness. He believes too little is done within all layers of the organisation, too make employees aware of why security measures are the way they are. *“Yes we know that sometimes it [security measures] is inefficient [to productive work] and that it delays and that it makes work more complex and that these pop-ups of data classification are annoying, but this is why we do it.”* (P09, Recording, 00:25:46).

Effort and willingness to comply

A recurring topic addressed in the personal interviews was the effort and willingness, or the lack thereof, of employees to comply with the security policy active at Damen Naval. One interviewee shared his thoughts on why employees would potentially be less likely to comply with a strictly closed working environment: *“I think people would have the urge [to non-comply] because they feel restrained in their work due to security. Playing the [individual] responsibility card would increase compliance and involvement. I believe this would work better than punishing people when something goes wrong.”* (P07, Recording, 00:33:00).

P11 mentioned that the current environments are becoming cumbersome and difficult, which leads to people becoming frustrated, thereby minimizing their effort to comply, because they just want to do their job (P11, Justification recording, 00:20:45). *“If you drive somewhere and you can take a shortcut by cycling over the sidewalk, 9 out of 10 [people] will do so, because it is faster and easier to do than following the bike path and making a detour.”* (Recording, 00:21:10). The interviewee further argued that: *“the moment you make it cumbersome to implement security measures, there is a higher chance that people will not comply.”* (Recording, 00:21:30). P07 added that it is impossible to have everything closed or restricted, so it would be better to involve employees and change their minds about security, as well as their responsibility herein.*“In the beginning [7 years ago], work was done based on trust. People appreciate this. If you give people trust, they will behave responsibly.”* (P07, Recording, 00:32:32). Another interviewee mentioned that, eventually, it all comes down to discipline and behaviour of people, as with the wrong intentions it is almost always possible to do harm (P08). P14 described how employees feel demotivated by the security implications and that this poses a threat of non-compliance or even leaving the organisation. Improving user satisfaction, in IT but also in terms of the ‘soft’ side, is core for the organisation according to the interviewee (P14). Finally, P09 stated that if employees know what the risks are and why the security measures are the way they are, employees will handle data differently from intrinsic motivation. *“This will also prevent people from searching for by-passes as you are aware of why things happen the way they do.”* (P09, Recording, 00:32:54).

5.1.6. Security performance measurement/alignment

This subsection portrays the interview findings related to performance management of security measures. This performance management may be both overarching and specifically aimed at a single security field or security policy.

Security Operations Centre

The Security Operations Centre (SOC) is the team of cybersecurity engineers involved in the protection of the organisation. The SOC is part of the security field of monitoring & incident response, but is specifically addressed at the security dimension of performance management. In order to be able to respond to incidents, logging data should be available to monitor potential incidents. P02 describes that more parameters would be desired to increase monitoring.*"If you want to be more effective and more efficient, many more parameters need to be included in security measures. "we stop everyone at the gate and will examine everyone individually. We are not sure what we are looking for... If, on the other hand, it is known what you are looking for, e.g. knives, you can take a metal detector and only respond to those people that have metal detected."* (P02, recording 00:43:30). Another interviewee working on the SOC (P12) agrees that there is room for improvement in the logging of information, but he finds it even more important that the follow-up on the data is improved. *"It's nice to see a display with lights, but someone should also look at it to see if something turns red."* (Recording, 00:12:45).

The procedures and roles within the SOC were discussed. One interviewee mentioned that he was not acquainted with the official procedure for incident response (P05). He elaborated that most processes are ad-hoc, but that, depending on the incident, a tailored approach is used to resolve the incident. He does believe that more procedures should be implemented and used within the organisation to ensure a better-structured environment. When asked if a feedback loop was active in the process of incident response, the interviewee responded that he does not believe there to be procedures for this. However, the cyberteam does occasionally evaluate incidents to extract lessons learned. This is more ad-hoc and unstructured. *"For some companies, everything is structured and procedures need to be followed. For other companies, like Damen Naval, it is more of an ad-hoc and go approach."* (P05, Recording, 00:12:47). This contrasts the answer of another respondent who argued that there is an incident response procedure in which the handling of incidents is described (P02). Be this as it may, the same interviewee also mentioned that in practice, a procedure is not always followed for every incident. The respondent also argued that for employees who are not directly involved in the drafting of policies and procedures, it may be hard to find the correct documents. This is due to the outdated intranet and 'hidden' information exchange environment (P02). P05 did express that he was positive with regard to the freedom he has within incident response, as too many formal procedures slow down the response on incidents. Therefore, he believed that it should always be possible to *"..let security personnel do their work. Would you rather ensure the continuity of your organisation or adhere to procedures?"* (P05, Recording, 00:16:30).

Access: standard open or standard closed?

A recurring point of discussion during the interviews, was the discussion about access control. Even though this is closely related to both data classifications and the need-to-know/be principles, from a security performance perspective, the technical implications and consequences for security are addressed. Even though most of the interviewees responded that they perceive the 'standard closed' way of access control to be restrictive in some way (P03, P04, P06, P07, P08, P09, P10), a significant amount of interviewees would also agree that a 'standard open' would be worse (P03, P06, P09, P11). Instead, different interviewees proposed a role-based access control. P03 believes access control currently is too much focused on the individual, but he also stated that role-based access is not of sufficient maturity to be implemented at Damen Naval. P06 believes that the current approach to access control is effective, but should be optimised, as access rights are too static. There is no feedback on access requests, so hypothetically, more access rights may be given without the responsible authoriser knowing this (P06). The respondent was also unsure whether access rights are automatically revoked or altered upon finishing or leaving a project. P03 would also promote better oversight on access control and agrees with P04 and P06 that there is a lack of traceability and automation. Also, the manual authorisation process with emailing back and forth is not desirable, as *"security needs to be made as user-friendly as possible."* (P04, recording, 00:27:45).

The current policy in relation to access control is set too strict for some interviewees, as it directly conflicts with their business needs and the completion of projects. P09 stated that: *"It would be a shame if the one [security] would rule out the other [delivering ships on time and within budget]"* (P09, Recording, 00:08:10). Another interviewee gave an example of these two aspects conflicting:*"I heard from people who needed a small tool to use but this was locked. By the time IT or security approved the tool it was 3 months later and the tool wasn't necessary anymore."* (P07, Recording, 00:31:08). P09 did mention that some delays in access control are not always a security issue, as *"sometimes access is requested [too] late by the departments."* (P09, Recording, 00:16:45). According to P08, the new ICT manager of Damen Naval would prefer to only classify data instead of applications themselves, which would also benefit access control, as *"access control is then about controlling of data instead of controlling of applications."* (P08, Recording, 00:19:08).

5.2. Security governance performance indicators

This section aimed to relate the extensive interview data of the case study at Damen Naval with similar phenomena in related literature and converges towards operationalisable security governance performance indicators. Security governance performance indicators should either indicate the performance of policy or contribution to business goals, without impacting the other one or, preferably, be about the alignment between the two. Many of the extracted performance indicators are applicable to multiple security fields, and therefore not addressed in one specific security field only. This section, therefore, starts with the overarching security governance performance indicators and then moves towards the specific security fields of the case study. Where applicable, connections were made to overarching performance indicators.

5.2.1. Overarching indicators

Organisation-wide security and responsibility

1. **Recollection of business goals:** Considering that effective security governance is about the alignment between business goals and the security policy, it goes without saying that these individual pillars should be clear and understandable by the employees within the organisation. As a result, a performance indicator for security governance is the extent to which employees understand and remember the business goals and/or project goals of Damen Naval. During the interviews, respondents were directly asked about their understanding of these goals, so one way to measure the recollection would be to interview colleagues. A more scalable method would be to implement a survey, on-demand or in a given time.
2. **Recollection of security policy:** In line with the previous security governance indicator, the other pillar of security governance, the security policy itself, has a similar performance

indicator, but is then aimed at the extent to which employees understand and remember the security policy of Damen Naval. This can be measured the same way as the previous point.

3. **Task delineation between departments (Role setting and naming):** A recurring finding of the interviews, across multiple security fields, was the delineation of tasks and responsibilities between departments. Clear task and role delineation boosts efficiency and ensures empowerment of employees within their respective roles, therefore the degree to which task/role delineation is implemented, understood and supported within the organisation, is an indicator of security governance. Specifically for data classification and access control, the sub-indicators below apply. For both of these indicators, a leading role of the security department is required, both in clarifying the policy and in ensuring that the policy is known among employees.

   (a) **Clarity of role-setting data classification:** Data classification within Damen Naval is necessary for all types of information within the organisation. Setting the correct roles and expectations for who should label information and who should be responsible is important. Therefore, the role-setting performance indicator is concerned with the clarity of employees' roles, expectations and responsibilities regarding data classification.

   (b) **Clarity chain of actors for access authorisation:** Multiple employees were unaware of the responsible stakeholders involved in access control. An indicator that contributes to security governance for this security field, would be the extent to which the chain of stakeholders is defined and known among employees.

4. **Responsibility/ownership over data valuation:** A recurring finding of the interviews was that employees had different interpretations over who should value data, and, thereby, the protection of data (). A performance indicator for security governance is the extent to which ownership over data valuation and the security thereof, by means of a business impact analysis, e.g., the 'Confidentiality, Integrity and Availability' (CIA) is done.

Risk-based

5. **Cost-benefit analysis (P04) security measures:** considering the threat environment of Damen Naval and the security measures in place, an indicator for a risk-based approach is that the (potential) benefits, or losses prevented, outweigh the potential losses, or benefits missed. Even though a cost-benefit analysis (CBA) is generally expressed in monetary value, the risk also includes the likelihood of something happening and thus can be assigned to the 'risk-based' subsection. A deterministic way of a CBA is impossible to implement in security governance, as it is very dependent on risk and even uncertainties. James and Predo [40] describe multiple ways risk assessment can be incorporated in CBA, of which only the Monte Carlo simulation offers a practical way for analysing the overall risk [40].

Direction of acquisition and commitment of resources

6. **Inefficiency factor:** It is known that security measures impact productivity within the organisation. Employees can be less efficient with their time as they need to take certain security measures, e.g. classifying information, encryption, etc. The interview results showed that project controllers aim to account for some inefficiency in the work of engineers but acknowledged that it was hard to quantify exactly, as the latest projects were all considerably different from anything that was done before (in terms of scale, working

environment, restrictions, etc.). Based on this, a security governance performance indicator that measures the additional hours spent on security, shows the commitment of resources to security. If fewer additional hours are needed to do productive work, without security being negatively impacted, overall security governance is improved. Systematically and structurally evaluating the estimated time spent on activities with the actual time spent on activities, would - in the long run - result in a well-established inefficiency factor.

7. **Performance expectations labour force:** Employees are expected to reach project deadlines and be as productive as possible, but, at the same time have to deal with security measures that increase the time spent on work. When trying to fulfil both these expectations, something has to budge. If it's not security or productivity, it might result in an increase in pressure/stress (P14) or another negative impact on the employee and/or the organisation. Due to this, a security governance performance indicator is the extent to which expectations for employees are realistically set within the available resources (e.g. working time). The term 'realistically' would imply that dialogue between engineers, management and security is needed to determine what is realistic.

Conformance with internal and external requirements

8. **Compliance rate:** Arguably one of the most renowned and used indicators for security governance is the compliance rate, either to internal or external requirements. Many security governance frameworks have adopted compliance and it is a recurring term in literature reviews [39, 51, 29]. Compliance with internal and external requirements, or a set policy, can be an indicator of security governance, as it indicates to what extent employees adhere to the set regulations. However, the compliance rate is heavily dependent on the two lower-level indicators described below:

   (a) **Effort on compliance:** A factor that is highly relevant for the compliance rate, is the effort employees are required to undergo for reaching compliance. Beautement, Sasse, and Wonham [7] describe this in their paper 'the compliance budget'. If the costs for compliance are high, and the compliance budget of an individual is exceeded, i.e., the effort is too high, the employee might not comply anymore. This is supported by Fogg [26] who mentions that human beings are fundamentally lazy and therefore reluctant to (too) much effort.

   (b) **Willingness on compliance:** Compliance, or engaging in desired behaviour, works best if employees are willing to do so and if the needs of the individual are aligned with the business needs [7]. If the motivation to act in a certain way drops, employees are less likely to engage in target behaviour [26]. Keeping these lower-level indicators in mind, will make the compliance rate a better indicator for security governance.

9. **Security governance vision (alignment policy and requirements):** A recurring finding of the interviews was that the security policy of Damen Naval is bound by external regulations. These regulations were sometimes conflicting with the desired policy of Damen Naval. Good security governance should ensure that the security policy results in optimal security, with the least impact on productive work. If external regulations would impose security measures on the internal policy, that are either negatively affecting security or productivity (keeping all else the same) or a combination of the two, Damen Naval should be able to engage in dialogue about whether these external regulations are necessary or subject to change. Comparing any conflicts between the policy and

regulations can be considered a performance indicator. The way in which this comparison is done and how potential misalignments or conflicts are acted upon, defines the score of the indicator.

Security positive/conscious culture

10. **Familiarity with threat environment and risk culture:** An indicator for the security culture within Damen Naval is the extent to which employees are familiar with the threat environment that Damen Naval is operating within, as this forms the basis of why the security policy and requirements are in place. This indicator can be measured by means of tests and improved by awareness training and informative newsletters with the current state of affairs regarding the threat environment.
11. **ICT knowledge (understanding of ICT effects):** Interviewees mentioned that familiarity and awareness of the threat environment alone were not sufficient for a security-conscious culture. As IT plays an increasingly more prominent role in the day-to-day operations of organisations, knowledge of ICT becomes increasingly important (P08). An indicator for security governance performance is thus the extent to which the consequences of ICT and their security implications are understood by employees. The operationalisable measures for measuring and improving are similar to those of the previous indicator.
12. **Employee empowerment:** A recurring interview finding was that employees, especially engineers, would need to be empowered more to make security-conscious decisions (P03, P08, P12). It also means that a culture of risk should be in place in which employees make informed decisions based on the potential risks and the alignment with business goals. As an indicator, employee empowerment would be the extent to which employees are supported in making security-conscious decisions based on their own expertise and the external environment.

Security performance measurement/alignment

13. **Accessibility of protocols / procedures:** The security department of Damen Naval has policies in place for a variety of security fields, operationalised with protocols and procedures. These protocols and procedures describe how policies should be followed and how employees should behave - and thus - be compliant. In order for this to work, protocols and procedures should be easily accessible and used throughout the organisation. A performance indicator for this is the extent to which protocols and procedures are accessible, e.g., by the time or amount of clicks it takes employees to open them. Furthermore, statistics could be gathered on the amount and distribution of opens, as well as the time looked at them.
14. **Audit and oversight:** A security governance indicator for security performance measurement/alignment is the extent to which the execution of the security policy is audited and overseen by the authorised person/department. Operationally, audits will include, among others, the verification and sampling of whether data is classified correctly and to what extent authorisations of employees are in order.

5.2.2. Access control

1. **Oversight access rights:** The level of oversight regarding access rights and the procedure for granting/revoking access rights was discussed with multiple interviewees (P04, P06) and is a security governance performance indicator.

2. **Automation access rights:** The extent to which access rights are automated is an indicator for security governance on access control, as automated revoking and assigning (correct) rights to employees both improve security, as no rights are wrongly assigned to employees upon completion or cancellation of projects, as well as improving productivity, as no manual effort is needed.
3. **Clarity need-to-know and need-to-be principles**: The need-to-know and need-to-be principles were considered to be vague, unclear and open to interpretation. Therefore, these principles would not be able to contribute to mature security governance, as part of the security policy of Damen Naval. The extent to which these principles are clear, the boundaries in which interpretation of these principles is allowed and the adoption of these principles in the day-to-day operations, is an indicator for security governance.
4. **Facilitation of knowledge sharing:** Knowledge sharing was said to be an important aspect of a well-functioning organisation, in which intellectual property and expertise of employees is paramount for the continuity of the firm. Even though a trade-off exists around knowledge sharing [23], better alignment between the extent to which engineers can meet as well as share information, and the protection against data leakage, is required. Better knowledge sharing/transfer, whilst upholding similar security standards, will boost productivity and contributes directly to reaching business goals, and thereby, indirectly, to security governance.
5. **Time to authorisation:** A recurring issue with interviewees was the time it took to receive access to information or physical areas. Having the time to authorisation as a performance indicator will improve insight into the duration of the authorisation process and will contribute to making improvements measurable. In its turn, a shorter time to authorisation will improve project efficiency and will contribute to better security governance, on the premise that security standards are kept the same.

5.2.3. Data classification

1. **Traceability data classification:** Different interviewees were unsure whether information was classified correctly. As much information at Damen Naval is sent via email, statistics could be gathered on the distribution of the classification levels (P10). This could, in its turn, be used to measure performance, e.g., the percentage of unclassified information.
2. **Clarity/explainability of data classification:** Employees perceived the different classification levels to be vague and open to interpretation. Interviewees also had differing opinions as to what classification means and what the consequences of classification levels were. Considering that unclear and unexplainable data classification levels are conflicting with the aims of the security policy and arguably cause frustration and misalignment among the workforce, a security governance performance indicator is the extent to which data classification is clear and can be explained in the same way.

5.2.4. Monitoring & Incident response

1. **Proportionality resources to threat:** one key indicator for monitoring & incident response is that the available resources for monitoring and responding to incidents is proportionate to the threat environment and the size of the organisation (P05). This could be expressed in the number of employees (FTE) or the budget available for tools and employees.
2. **Proportionality response to impact:** Employees responsible for cybersecurity and incident response argued that the response to an incident should be in line with business

values, requirements and the external environment (P13). The extent to which this is done, is an indicator for security governance performance.

5.3. On the road to concordance

This section describes the outcomes of the focus group session. The security fields of access control and data classification were discussed first. Afterwards, participants were asked about conformance to (external) requirements. Finally, the road from compliance to concordance was discussed, using the doctor-patient relationship as a metaphorical analysis.

5.3.1. Data classification

The different data classification levels of Damen Naval were discussed. Respondents were asked to respond on the 'Titus' plugin that is used for classifying data. The plugin describes the data classifications as the following:

- DSNS Public: not harmful
- DSNS Internal / commercial in confidence (external use): considerably harmful
- Damen Schelde Naval Shipbuilding Restricted: seriously harmful
- Damen Schelde Naval Shipbuilding Confidential: catastrophically harmful

DSNS Public was considered to be a straightforward classification. Participants agreed that this was information that was not harmful, as one participant mentioned it 'could be left at a bus stop' (G01). DSNS internal / commercial was perceived as the standard for communication (G02). G03 added to this that this concerns information that you do not want to wander on the street, with commercial in confidence being used for information that is to be shared externally and internal for information that shouldn't be shared externally (G03). G04 believed that restricted is information that everyone within a single department should be able to read and confidential comprises information that only specific individuals or a very select group of people should have access to. G02, on the other hand, would argue that both restricted and confidential are classifications that everyone working on a project should be able to see, unless there are specific rules in place that state otherwise (G02). Based on his role of a technical specialist, he argued that even though information is confidential and comprises military sensitive information, the entire project team should be aware of this information as it contributes to a successful product (G02).

G03, a representative of the security department, argued that having access to something is different from what classification information should have. "*Classification is about how to protect and secure information, which can be entirely different from who should have access.*" (G03, Recording, 00:12:40). He further stated that *"a document that is [classified as] DSNS restricted is protected in a certain matter, but still the entire organisation may have access if they all need access."* (G03, Recording, 00:12:54). Following this reasoning, other participants agreed that classification and access are separate things. G04 did state that, although agreeing with the argument, that classification is - in practice - commonly intertwined with access control. *"If something is about classification, the first question is: how do I get it [information]? We want to be able to use it, so therefore these two concepts are similar to us."* (G02, recording, 00:15:00). Based on the discussion and the elaboration of the intended definition of the classifications, participant G04 stated that he wanted to nuance his initial definitions by stating that *"..classification labels are the value or the potential damage of a document."* (G04, recording, 00:16:32).

Participants of the group session then discussed the consequences of data classification. G03 stated *“with confidential it will be made very hard to get access, but this is unrelated from whether you should get access to it.”* (G03, recording, 00:17:02). G05 adds to this that making it hard is not necessarily the case, as this depends on how the controls are currently implemented and what could be done to improve. From a practical ’business’ viewpoint, G02 responded that this might be a threshold for people to get access, as it is made to hard for them. The participant even argued that this could negatively impact security itself: *“Because it is so hard [to get access], people expect me to tell them this confidential information in an environment that is not confidential, with the risk of them writing it down and it [information] going into the restricted network.”* (G02, recording, 00:17:47).

During the discussion on data classification, the classification family of Damen Naval data was used. However, multiple other classification families exist. These classification families can be project-specific. G02 states that he tries to relate the different classification families back to the classification family of Damen Naval. *“In my head, I try to relate the client classifications to DSNS classifications and in 95% of the cases this is possible. This way I only have 5 classifications to remember instead of … 15 [due to different projects].*” (G02, Recording, 00:20:06). Participants were in agreement that the different data classification families should be kept separate in practice.

As part of the group session, participants were asked to give their opinions regarding data classification on the pictures below. First, the left picture of figure 5.1 was shown. Participants were in agreement that this picture does not contain any information that should be classified. G02 gave a more detailed explanation of why this information may be publicly available: *“…if the ship is done, everyone can see it so it is not that tensive anymore. We are also not in a competitive position anymore as the contract is already signed, so I believe the design can be released.”* (G02, recording, 00:23:51).

Next, the participants were shown the same image but now with detailed information about suppliers, weapon types and general characteristics of the frigate (image on the right side of figure 5.1). Again, most participants felt that there is no real breach in data classification, as most information is publicly available on Wikipedia (G01). G02 even responded by saying that both pictures are the same to him, as he can distinguish the suppliers and systems based on the first picture. *“Someone who knows a little bit about ships has enough of the drawing alone.”* (G02, recording, 00:27:03). G04 would go as far as stating *“Everything that is publicly visible from the outside can per definition not be classified.”* (G04, recording, 00:27:20). The participants were in agreement that despite this information being publicly available now, Damen Naval should be in control when information is made public. On the one hand, Damen Naval does not want to release information prematurely if a contract has not been signed (G01). On the other hand, releasing the information could steer others into using the correct information, thereby preventing wrong information that might endanger contract negotiations (G04).

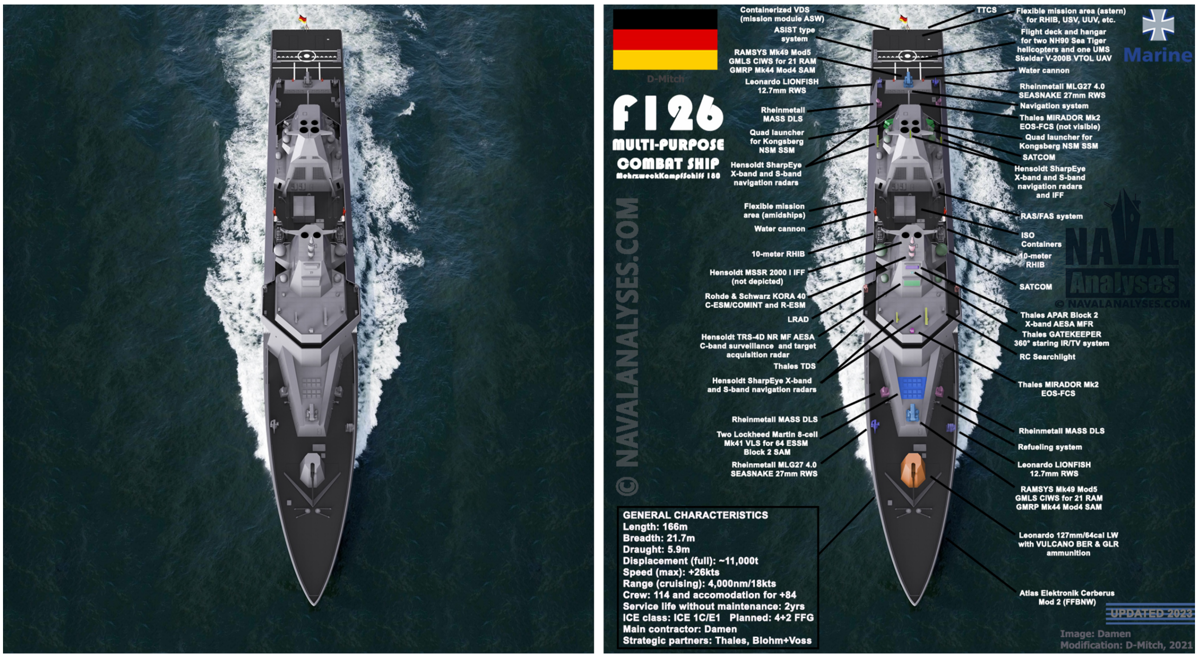

D-Mitch
F126
MULTI-PURPOSE
COMBAT SHIP
MehrzweckKampfSchiff 180
© NAVALANALYSES.COM
Containerized VDS (mission module ASW)
ASIST type system
RAMSYS Mk49 Mod5 GMLS CIWS for 21 RAM GMRP Mk44 Mod4 SAM
Leonardo LIONFISH 12.7mm RWS
Rheinmetall MASS DLS
Quad launcher for Kongsberg NSM SSM
Hensoldt SharpEye X-band and S-band navigation radars
Flexible mission area (amidships)
Water cannon
10-meter RHIB
Hensoldt MSSR 2000 I IFF (not depicted)
Rohde & Schwarz KORA 40 C-ESM/COMINT and R-ESM
LRAD
Hensoldt TRS-4D NR MF AESA C-band surveillance and target acquisition radar
Thales TDS
Hensoldt SharpEye X-band and S-band navigation radars
Rheinmetall MASS DLS
Two Lockheed Martin 8-cell Mk41 VLS for 64 ESSM Block 2 SAM
Rheinmetall MLG27 4.0 SEASNAKE 27mm RWS
GENERAL CHARACTERISTICS
Length: 166m
Breadth: 21.7m
Draught: 5.9m
Displacement (full): ~11,000t
Speed (max): +26kts
Range (cruising): 4,000nm/18kts
Crew: 114 and accomodation for +84
Service life without maintenance: 2yrs
ICE class: ICE 1C/E1 Planned: 4+2 FFG
Main contractor: Damen
Strategic partners: Thales, Blohm+Voss
TTCS
Flexible mission area (astern) for RHIB, USV, UUV, etc.
Flight deck and hangar for two NH90 Sea Tiger helicopters and one UMS Skeldar V-200B VTOL UAV
Marine
Water cannon
Rheinmetall MLG27 4.0 SEASNAKE 27mm RWS
Navigation system
Thales MIRADOR Mk2 EOS-FCS (not visible)
Quad launcher for Kongsberg NSM SSM
SATCOM
Hensoldt SharpEye X-band and S-band navigation radars and IFF
RAS/FAS system
ISO Containers
10-meter RHIB
NAVAL Analyses
© NAVALANALYSES.COM
SATCOM
Thales APAR Block 2 X-band AESA MFR
Thales GATEKEEPER 360° staring IR/TV system
RC Searchlight
Thales MIRADOR Mk2 EOS-FCS
Rheinmetall MASS DLS
Refueling system
Leonardo LIONFISH 12.7mm RWS
RAMSYS Mk49 Mod5 GMLS CIWS for 21 RAM GMRP Mk44 Mod4 SAM
Leonardo 127mm/64cal LW with VULCANO BER & GLR ammunition
Atlas Elektronik Cerberus Mod 2 (FFBNW)
UPDATED 2023
Image: Damen
Modification: D-Mitch, 2021

Figure 5.1: Left: clean picture of an F126 frigate [8], right: infographic of F126 frigate [17], both publicly available

The participants of the group session were asked whether they perceived there to be a trade-off or balancing act between the usability of information and the security of that information. In line with what was said earlier, participants mentioned that this depended on whether data classification itself would impact accessibility (G01, G04). G01 stated *"If you only label [classify] this does not make you handicapped."* (G01, recording, 00:32:12). G04 added to this that there might also be solutions that improve both usability and security. Another participant considered this trade-off to be much more framed, as he described: *"the security or the value of documentation is something that is given or required by the client. Then, we should consider how to make this as usable as possible, considering these prerequisites."* (G02, recording, 00:32:43).

This being said, participants agreed that a trade-off could be made to a certain extent. G05 gave an example of how data classification and security may be perceived as obstructive, when, if another label was put on the information, the usability could have been improved. In line with this, G04 mentioned that a conservative classification policy, wherein everything is classified as DSNS confidential, might be an improvement for security, but will impact usability as classifying will cause impediments in using the information. G03 proposed costs to be an additional factor in the trade-off, whilst G02 argued that this is more related to access control, as the costs as well as how people classify are related to access control. *"People will under-classify information if they otherwise have to walk to the confidential laptop."* (G02, Recording, 00:36:08). The other way around, *"Other people are so afraid of doing something wrong [leaking information], that they over-classify."* (G02, recording, 00:36:19). This would indicate that there should be a balance between usability (classifying low) and security (classifying high). G03 agreed with this statement.

As a final point related to data classification, the discussion of who should classify information and be responsible for it. Even though participants would agree that engineers are the most suitable for determining how confidential information is, based on their technical expertise, they would also agree that engineers do want to focus on their engineering work rather than classifying information: *"...90% of the employees are engineers who want to calculate steel plate thickness or the amount of air that needs to be circulated within a room. They don't want to worry about the label to put on it."* (G01, recording, 00:37:20). In an attempt to lower the potential burden on engineers, G04 asked whether templates would improve the situation. G01 and G03 responded that this is partly being done by the PDAL (Project Document and Activity List), but all participants agreed that setting everything in templates would negatively impact the 'thinking for yourself' approach and the autonomy of engineers. *"..thinking should be stimulated, because we [the business] have to deal with it [classification]."* (G02, recording, 00:40:40). He did argue that more involvement for responsibility over data classification should be expected from team leaders (G02).

5.3.2. Access control

The second topic was the security field of access control. The principles of need-to-know and need-to-be were briefly elaborated. The internal security plan of Damen Naval stated the following on the need-to-be principle: *"access to areas where one should be for executing his/her working activities."* [63] (p. 28). No specific description was found on the need-to-know principle. Afterwards, the participants were asked whether there was a need-to-be in the following statement: *Due to workplace shortages the intern is given a workplace on a project floor despite not working on the project itself.*

Respondents disagreed on whether there was a need-to-be in the case of the intern. G04 believed there to be a 'practical yes' and indicated that *"in the balance this statement slides towards usability instead of security."* (G04, recording, 00:41:35). G02 would agree with G04 on the prerequisite that *"the intern should at least have a screening or undergo the same measures as others on the project have to undertake."* (G02, recording, 00:41:50). G01 was against the statement, as she would not agree to let the intern on the project floor.

G03 believed that*"eventually the question should be if you need to be on the project ... this would mean the information, the knowledge, the designs that are made or the people that work there."* (G03, recording, 00:44:01). Following this description, participants were asked what this 'need' was. G03 states that the need-to-be is not as simple as it is sometimes perceived. *"The need-to-be sounds very simple, but eventually it still comes down to a scale with how strict this policy needs to be set. Very strict so that nobody has access anymore; this is good for security but bad for productivity, or less strict so that you can talk with colleagues."* (G03, recording, 00:46:50). G04 and G01 believe that there could be a need in the situation of the intern, but *"due to workplace shortage should in no way, shape or form be a need."* (G04, recording, 00:45:43).

Finally, respondents were asked how the security policy regarding the principles of need-to-know and need-to-be is currently set and whether this policy leans more towards security or accessibility/usability. Two of the participants (G01, G04), believed the slider to be more set towards security in policy. However, in practice, opinions differed. G04 believed that steering on risk acceptance might overrule the need-to-be or need-to-know principle, but G01 argued that this might give wrong impressions to an intern as in practice the policy is not adhered to as the policy said it would. She argued that the slider should be closer towards security, i.e., that the intern should not be on the project. *"We want to give new employees the feeling that we do it seriously over here. We build warships."* (G01, recording, 00:50:40). In contrary to the theoretical policy, currently, Damen Naval is leaning more towards usability/accessibility, as in practice people do get access whilst the policy would suggest otherwise (G05, G01). Overall, G02 believed that everyone [limited to the participants] is generally speaking on the same line. He did suggest that need-to-be is hard to demarcate and should always be open to some interpretation.

5.3.3. Conformance to requirements

The group session's third topic was conformance to (external) requirements, as this was a common point of discussion during the individual interviews. The following statements were used to start the discussion about these requirements:

1. The way in which Damen Naval conforms to external rules such as the ABDO is open to interpretation.
2. The internal security policy (beveiligingsplan) is based on / a derivative of the external regulations imposed on Damen Naval (e.g., ABDO)

G03 mentioned that *"the requirements in itself are quite strict, but the way in which these requirements are satisfied is open to interpretation."* (G03, recording, 00:55:26). The participant partly agreed with the second statement, as the internal security policy of Damen Naval is partly derived from external requirements such as the ABDO. G03 explained that this had to do with the core of the business working on projects bound by these regulations. The participant did mention that "at the same time you also have your [Damen Naval] own interests, which is the full responsibility of Damen Naval and risk-based." (G03, recording, 00:56:34). He argued that the internal policy is not a direct copy of external requirements. G04 did not agree with this, as he believed that Damen Naval should have a more clear distinction between the DSNS information and client information, as some of the internal policies rely too much on external requirements (G04).

Afterwards, the question of whether Damen Naval should conform to all external requirements at all was addressed. G03 was clear in stating that:*"We don't have to do anything … Eventually the MT says that we want to build navy ships and if we do not apply to these requirements, the risk gets very high that we do not get the project."* (G03, recording, 00:58:24). G03 followed up on this by saying that only those with a position of power that are able to weigh different interests can decide whether to comply or not. However, G02 believed that weighing these interests is not something that can be done as an individual, director or not. According to the participant, considerations of the project floor should always be taken into account.

In line with the statements about conformance to requirements and the nature of the research, G02 stated that: *"we are sometimes so busy asking security what to do that we forget that we also need to build a ship."* (G02, recording 01:06:12). He explained that a group of people from security and IT are looking at what needs to be done to create a secure environment, but engineers look more at what their need is. He argued that the different departments do not communicate well enough. *"…instead of asking the question that something needs to be restricted, we should also ask the question how to do something given the rules."* (G02, recording, 01:06:58). Weighing between needs and requirements is something that should be considered continuously (G02). Other participants agreed that better alignment is required. G03 concluded by stating that security, IT and other departments are supportive of the business which makes better alignment essential.

5.3.4. Doctor-patient relationship applied to Damen Naval

Having discussed some key operational issues that impact either or both productivity and security, the final part of the group session intended to look at this balancing act from a more generic perspective with the aim of reaching a state of concordance, or at least agreeing on a path to take to reach concordance at a later stage. In doing so, the doctor-patient relationship (as described in section 3.1) was used as a metaphorical analysis to project upon the organisation of Damen Naval.

The first question that was proposed to the participants was whether a doctor-patient relationship would be applicable to an organisation like Damen Naval. G02 considered the doctor-patient relationship as difficult to implement, as the organisation of Damen Naval does not work with a single doctor-patient relationship, by stating: *"a project with 500 people is not suitable for asking each individual engineer what his best approach would be as this results in 500 individual plans."* (G03, recording, 01:12:46). This is a logical concern that was shared by more participants, as the paper by Vermeire et al. [66] did mention that *"Knowing each patient's health beliefs is the key feature of the new doctor-patient encounter."* (p. 340).

G02 argued that the business must still have a leading role in setting a policy, as *"even if there are strict rules, the engineer will find his own solution."* (G01, recording, 01:13:03). This was complemented by the example of G04: *"There is a business need for exchanging information. This is done via google drive. IT blocks google drive. The business still needs to exchange so will use Yahoo drive. Then Yahoo drive is blocked. Eventually, this ends with Yahoo.ru.*" (G04, recording, 01:18:36). This does align with the shift of the doctor-patient relationship from compliance towards concordance, as *"The backbone of the concordance model is the patient as a decision maker"* [66] (p.333). Acknowledging that when pursuing compliance of employees, employees can still choose not to comply, is something that was clear among the participants. Apart from the viewpoint of the individual, the same rationale was also used when compliance versus concordance was discussed from an organisation-wide level: *"the doctor advises on what the patient should do to become better… the decision to follow this advice is with the patient. Seeing the patient as the business, the business should eventually decide what to do and what not."* (G03, recording, 01:17:45). This is strongly related to the previous subsection.

In line with this, creating awareness and showing why certain measures or requirements are necessary is an important factor (G01). During the group session, she used the metaphor of a mother-child relationship to explain why certain measures are necessary. *"I want to explain to my children why they need to brush their teeth, hoping that they will do it on their own, as holes in your teeth are not so funny."* (G01, recording, 01:13:22). Followed by: *"this is why you need to create awareness among employees as to why follow what is said [by the security department]."* (G01, recording, 01:13:33). Related to the doctor-patient relationship, this can be explained by patients having to believe that they are vulnerable and that there is a necessity to adhere to a set of health recommendations in order to lower the severity of the threat [66].

Apart from the shift from compliance to concordance, participant G04 would rather pursue being in control. According to the participant, compliance is always doing what should be done, in which deviation is not possible. In control, on the other hand, is about finding a solution to a problem, together, based on the necessary risk assessments and conscious considerations (G04). Reaching concordance is then, according to the participant, closely related to becoming in control. Even though the names might differ, after the discussion, participants were aligned in their basic definition of concordance.

Based on what was said earlier during the group session, participants were asked how they would see a structure for concordance work within the organisation. Participant G02 described a project structure involving working groups and steering committees, with engineers that have field knowledge, advising the steering group on a higher level. This steering group then decides on the matters at hand. The participant mentioned that such a structure would be able to leverage the specific knowledge and input of individuals, whilst also enabling decision-making. *"This would be exactly what you want [as an organisation] as this involves different expertise combined to come to a good solution, with the steering committee making the decision on the right level [of authority].* (G03, recording, 01:21:23). After additional elaboration by the participant, the steering committee receives input from lower down, usually via team leads or directly from engineers, but not all input was said to be brought up during the meeting as individuals were said to filter some of the input. Issues are collected and then decided top-down by the steering committee instead of advice being given first by the working group. The other participants agreed that in principle this would be a good structure to pursue concordance (G01, G03, G05). G02 added to this that the whole line would have to be included, with representatives of all stakeholders. Currently, this is not the case, as, among others, the security department is not involved.

Finally, the role of the client of Damen Naval is discussed in the context of concordance. G02 stated that this role is given, as the client and the requirements are there to be dealt with. G01 argued that *"the client is interested in getting the right product [ship] and has drafted some requirements for this, but he will also tinker with these requirements if he doesn't get the desired product when asking it in this way to the business [projects Damen Naval]."* (G01, recording, 01:24:07). This would indicate that a potential client might alter the requirements if requirements are too strict for any shipbuilder to take on the challenge. G04 agreed with this but also mentioned that it works the other way around as well. According to him, it is possible to convince the client of another way of working or another approach which he hadn't thought of before. Likewise, G02 would also argue that some form of freedom over requirements would be possible: *"I would be a proponent of that the client tells what he wants but not how he wants it to be done."* (G02, recording, 01:26:10).

5.4. Converging towards a framework for determining the maturity of security governance

The previous sections answered the sub-questions for this research and contributed to shaping the framework for determining mature security governance. This section converges towards the framework for determining the maturity of security governance. The research addressed maturity both from a conventional field of view, as well as through a social lens. Conventional maturity focuses on the effectiveness of security governance and is more technically oriented. This side of the framework consists of the six dimensions of security governance that were extracted from the literature review. Based on these dimensions, indicators were created that can be used to measure the effectiveness of security governance. The dimensions and indicators should not be mistaken for indicators to improve security per se. Instead, this part of the framework is also concerned with governance, be it from a different perspective than social maturity. A higher maturity level would either or both increase the security policies or the contribution to business goals, by working more productively/efficiently given certain security policies. It is thus not merely about implementing technical measures to protect systems and assets. The framework is shown in figure 5.2.

The other part of the framework considers maturity to be a social construct. It focuses specifically on the way alignment between the two pillars of security governance, i.e., security policies and contribution to business goals, is reached. Socially mature is used metaphorically within the research as it indicates a state of human development characterised by people becoming more conscientious, responsible and agreeable with age [58]. The highest notion of this social maturity is defined as reaching concordance. The framework, therefore, visualises the shift from compliance to concordance. One important aspect to take note of is that eventually the security department or the higher management has to impose the outcomes of the stakeholder dialogue into a policy. Otherwise, there is no way forward from this dialogue. An interviewee from the group session referred to this as being ’in control’ as opposed to being compliant or demanding to be so. This indicates that apart from a bottom-up approach, eventually it also entails a top-down approach and an agreement about how this newly formulated approach will be adhered to. This is why the framework also has an arrow down from concordance to compliance, as it indicates that, although drafted in concordance, employees need to be compliant with whatever the outcome is.

Both the conventional and the social maturity side of the framework are linked by security governance trade-offs. The second sub-question of this research aimed to understand what type of trade-offs related to security governance there exist within organisations and if this was supported by the challenges employees at Damen Naval perceive. The conducted interviews showed that employees at Damen Naval are confronted with a variety of challenges and trade-offs. Some issues can be resolved by focusing on the security governance dimensions and its derived performance indicators. Others, however, are more wicked and social problems, that do not have one best solution that can be imposed upon employees top-down. Instead, they require a dialogue with representative stakeholders to openly discuss what the optimal way forward is.

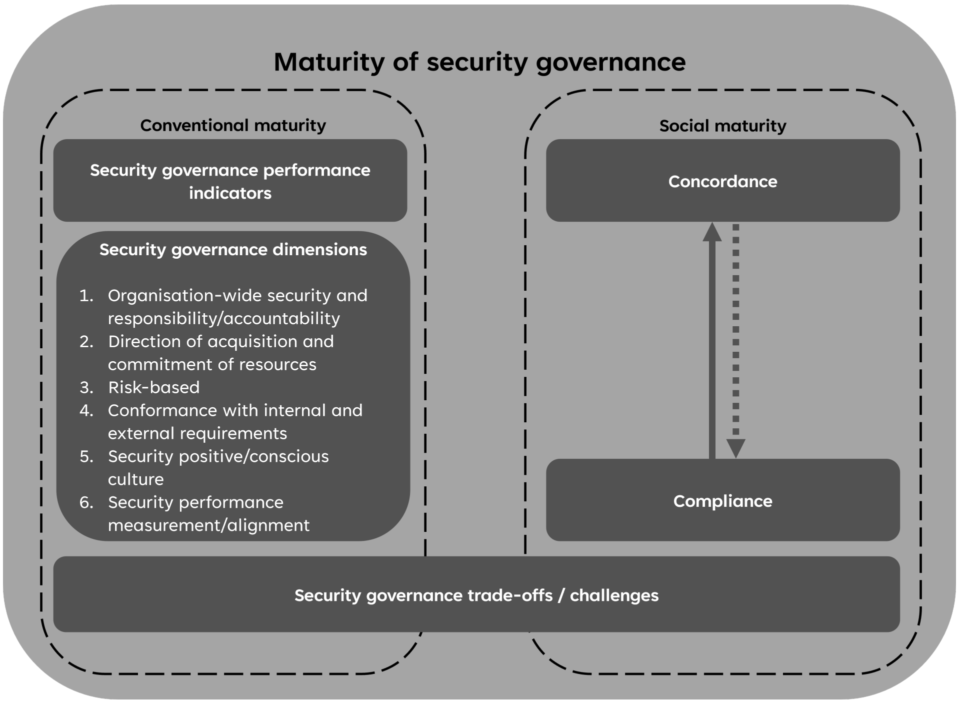

Maturity of security governance
Conventional maturity
Security governance performance indicators
Security governance dimensions
1. Organisation-wide security and responsibility/accountability
2. Direction of acquisition and commitment of resources
3. Risk-based
4. Conformance with internal and external requirements
5. Security positive/conscious culture
6. Security performance measurement/alignment
Social maturity
Concordance
Compliance
Security governance trade-offs / challenges

Figure 5.2: Developed framework for determining the maturity of security governance

6 Discussion

This research has provided insight into the world of organisational security governance. The outcomes of this research have provided a framework for determining the maturity of security governance, both from a conventional viewpoint on maturity as well as a social viewpoint. Both sides of the framework require challenges and issues of security governance as perceived by individuals or groups within organisations. The conventional side of the framework aims to solve these issues and challenges by means of security governance performance indicators, derived from a selection of dimensions along which security governance can be assessed. These dimensions were used as a base for semi-structured interviews on three individual security fields with a broad representation of employees at Damen Naval. After a thematic analysis of the interviews, security governance performance indicators were drafted that are able to be operationalised into measuring the maturity of security governance on either the individual security fields, or overarching security practices.

Finally, the social maturity of security governance was addressed by discussing the challenges and trade-offs that individuals perceived during the interviews. The social maturity viewpoint acknowledges that not all perceived issues in organisational security governance can be solved by one single solution. Instead, they require dialogue with a variety of stakeholders and their expertise/opinions. By means of a focus group session (based on the theoretical framework of chapter 3) participants could discuss some of the most pressing challenges employees faced at Damen Naval, as they were asked to debate about trade-offs between both sides of security governance. The final aim was to set trade-off sliders or at least agree upon the right way forward by determining how concordance can be reached within the organisation of Damen Naval.

This chapter provides the major findings of the results section and interprets them based on initial expectations, the context of the literature review and theoretical framework, as well as an evaluation of any unexpected results and their significance. Next, the limitations of this study and the potential consequences are discussed, as well as their implications for interpreting the results. This chapter concludes with recommendations for future research.

6.1. Major findings and their relation to theory

6.1.1. Issues related to security governance

One of the main issues extracted from the interviews has to do with role setting and responsibilities. Interviewees from the security department were not completely aligned in their roles, tasks and responsibilities. On top of that, the role setting of the ICT (cyber)security department and the security department were indistinct. A possible explanation for this is that the phenomenon of cyber-physical systems has intertwined physical security and cyber security [52, 11]. This led to the blurring of ICT and security aspects and could explain why the role setting between these departments at Damen Naval is unclear. Another factor that could contribute to this is the significant business growth that Damen Naval went through in a very short time.

Due to the scoring of multiple large projects with strict regulations, Damen Naval grew harder and faster than the organisation could comprehend. This led to a serious backlog in ICT projects (subsection 5.1.3, but also imposed a lot of pressure on the engineers (subsection 5.1.3). Even though the additional burden on employees was acknowledged by management and business controllers, engineers were still motivated to spend fewer hours on working activities than necessary. Interview results indicate that engineers would absorb some of the additional costs of the security requirements in their working activities, which would impose additional stress on them. In principle, this issue does only impact productivity. Be this as it may, indirectly, this is also a driver for non-compliance as the high resource investment that these security measures demand conflicts with the completion of their primary task [44]. This is also in line with the paper by Beautement, Sasse, and Wonham [7] and point three of the framework about secure behaviour of Sasse et al. [59].

Another interesting result is the broad interpretability of the internal security policy. During interviews, respondents had varying interpretations of security principles as need-to-know and need-to-be, as well as conflicting understandings of data classification (subsection 5.1.4). Based on the analysis of these results, it can be concluded that the ’need’ for the principles for access control lacks clarity in the policy (subsection 5.3.2). Furthermore, respondents couldn’t agree on specific cases of the principles and argued that there should always be a possibility for interpretation, which begs the question if - at all - the ’need’ can be defined unambiguously in a security policy. This refers to the trade-off by Gulzar and Kopcho [32] about rules and principles, as discussed in section 2.4. The principles of need-to-be and need-to-know aim to leverage competence and context by the decision-maker, i.e., the respective employee, instead of enforced compliance to a rigid rule [32]. Even though this rules-principles theory is preferred to be more towards the principles side, Damen Naval lacks the proper authority or empowerment of the decision-maker. Setting a principle-based security measure for access control, is beneficial if the respective employee has decision-making rights. However, in practice, the process for access control to information and/or environments constitutes of different stakeholders and is perceived to be too static and strict (subsection 5.1.6 ’Access: standard open or standard closed’). Contrary to the benefits a principle-based policy should attain, this is currently not realised within Damen. Kirlappos, Beautement, and Sasse [44] argues that *”Greater flexibility is needed to adapt to local circumstances, and solve conflict with tasks and business processes as they arise.”* (p.77). Although greater flexibility may be a suitable option, it should also mandate that employees can execute and make decisions based on their interpretation. Otherwise, it will only frustrate employees as their interpretation of the principle is not shared and executed by others who do possess this decision-making right.

In addition to access control, data classification was also considered to be a 'grey area' in terms of interpretation of the policy. During individual interviews and the focus group session, employees proposed different descriptions of the DSNS classification levels to make them more relatable and practical to employees, which indicates that the current description is too vague and hard to distinguish from one another. Interestingly, multiple respondents related data classification directly to access control. Nonetheless, a representative of the security department explained that these two are separate things, as defining how to protect information is entirely different from defining who should have access (G03, subsection 5.3.1). After this explanation, the other participants of the group session agreed that data classification should be interpreted accordingly. These findings show a lack of understanding of the policy. Considering that the security policies regarding data classification, as well as the tool that is used to classify data, only vaguely describes what each classification means, the security department could do more to clarify this policy and explain the differences between access control and classification. Understanding of the policies is part of the awareness maturity curve by Sasse et al. [59]. Building understanding beyond the secure routine of merely classifying information, improves security awareness [59].

It is important to add that the clarity of classification levels was not the only aspect hampering data classification. Results of the individual interviews show that even engineers with specific expertise were not completely reassured about classifying something in a certain way, whilst others would classify most parts of the ship on a very low level (subsection 5.1.4). This suggests that no consensus or unilateral assessment criteria can be applied to classifying information. Nevertheless, the focus group session showed that many highly classified systems are already public information (on a very high level) and would indicate that, at the corresponding level of detail, this information cannot have a high classification anymore (subsection 5.3.1). This does, at least to a certain extent, proposes a practical way of determining the appropriate classification level.

Results of the interviews as well as the focus group session also point to ambiguity and disagreement about the responsibility and accountability of classifying data. Even though some respondents had conflicting opinions regarding who should classify information, overall participants agreed that engineers are the most suitable for determining how classified information is, due to their technical expertise (section 5.3.1). Representatives of the engineering department did mention that engineers do not want to worry about putting a label on data as it is in stride with their primary tasks of doing actual engineering work [44, 59, 7]. In trying to reduce the time spent on data classification, it is very much possible that engineers do not always classify data correctly. In addition to this, currently, the accountability of data classification is assigned to the data owner, which, in most cases, is the engineer. Interview results indicate that data is classified too high more often than too low, which can be explained by the accountability of the engineer.

In addition, the results show that those who are negatively impacted by classifying a document too high, are often not the same employees as those who classify the data. This relates back to section 2.1.4 in which Anderson and Moore [3] was quoted, stating that *"Systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail"* (p. 610). The system, in this case, is the policy of data classification. The person guarding it, is a metaphor for the engineer who needs to classify correctly and the one who suffers is the project leader or manager who is impacted by the measures that follow from a higher classification than necessary. All of this points to the conclusion that the policy of data classification is flawed due to misunderstanding of the classification levels, misalignment with primary tasks as well accountability and consequences.

A final topic to depict from the research results is the conformance with internal and external requirements. Apart from being one of the chosen security governance (subsection 2.2), requirements play a critical role in the security policy and the way this policy is perceived by employees, as well as their willingness to comply. Results of the individual interviews indicate that many of the issues that impact productivity are present due to externally imposed restrictions. Some of the interviewees mentioned that conformance to requirements is a necessity for making ships (subsection 5.1.4. Considering that security governance comprises alignment between the security policy and business goals, one could argue that if conformance to requirements is a necessity or precondition for executing projects, conformance is already part of the business goals itself. Other interviewees believed there to be more flexibility and interpretability in the way imposed restrictions are implemented at Damen Naval. This was supported by the findings of the focus group session (subsection 5.3.3). Existing literature does not seem to take this interpretation of requirements, to better fit with business objectives and productive work, into account. Most frameworks and norms emphasise that compliance to requirements should be ensured, without any notion of interpretability or support by employees [29, 51, 39]. Westby and Allen [68] do mention that requirements should be supported by people upon implementation, but does not show any active involvement of the business for drafting requirements.

It is also worth noting that the results of the interviews showed a difference between external regulations and internal regulations. For a set of internal requirements that is decoupled from any imposed external requirements, Damen Naval can align and adapt regulations to business needs and desires of the employees. This means that internal regulations are more easily changed or better explained. External regulations, however, were said to be very static and outdated. Even though Damen Naval complied to these external regulations, it would arguably negatively impact both security and productivity. One example of this, is the use - or the lack thereof - of cloud services (subsection 5.3.3, p.38). The interview results indicate that employees find it frustrating and hard to comply with such a regulation. Due to this, it is very much possible that the costs and benefits of adhering to these external requirements are out of balance. Especially from the viewpoint of an engineer within the organisation, as productivity gets impacted, but it arguably is also more costly against a lower level of security. Based on the results of the interviews, the only thing that keeps this imbalanced way of working afloat, is that employees deem it necessary for the continuation of projects and thereby the organisation itself.

6.1.2. Performance indicators

The results of section 5.2 show that most security governance performance indicators are applicable to multiple security fields. In the research design, three different units of analysis were chosen: access control, data classification and monitoring & incident response, in order to relate the performance indicators to one another and to understand to what extent the indicators were generalisable. In this section, indicators are discussed and related to existing theories about security governance.

First and foremost, the results of the individual interviews indicate that the majority of the interviewees are familiar with the business goals of Damen Naval. Almost every respondent who was asked to give their interpretation of the business goals answered that in principle it was about delivering [complex] ships on time and within budget, which aligns nicely with the business plan of Damen Naval [18]. This is important as it is one of the pillars of security governance, i.e., the alignment between (contribution to) business goals and security policy [2]. Both the recollection of business goals and the recollection of security policies are considered to be overarching performance indicators for security governance.

The other two security performance indicators are concerned with the task delineation between departments and the responsibility over data valuation. Interview results show that the lack of role-setting and naming caused departments to be misaligned. Specifically for the security policy, this caused discrepancies between the security and the ICT department. Together with the lack of clear ownership over data valuation by means of a business impact analysis, these indicators would score somewhere between level 1 and level 2 when relating them to the maturity framework by Maleh et al. [48]. Level 3 in the framework mentions that *"IT and some other business units have agreed-on IT component and physical environment security measures."* ([48] (p.227)), as well as *"Security incidents are handled based on the urgency to restore services, as agreed on by IT and some other business units."* ([48] (p.227)). The lack of a clear and structured business impact analysis prohibits security incidents to be handled based on the urgency to restore it, and the lack of alignment between the security department and the IT department disputes the first statement for level 3 maturity. Although this performance indicator concerns the whole security policy, specific performance indicators were assigned to the security field of access control and data classification.

The following three performance indicators relate closely to each other and are applicable to all three security fields. The first indicator is a cost-benefit analysis based on the security measures. Interviewees, including those from the financial department, could not quantify or compare within reasonable accuracy how the (potential) benefits - or losses prevented - outweighed the potential losses - or benefits missed - from the active security measures. Interviewees could give examples of how security measures impacted the productive work of employees by assigning additional hours spent on security for working activities, which corresponds with the efficiency factor indicator. Interviewees mentioned that the inefficiency of additional hours spent on activities due to security measures should partly be absorbed by the engineers themselves (subsection 5.1.3, p.36). When no thought is given to performance expectations of engineers, i.e. if engineers are expected to deliver the same productive work whilst consuming the same amount of resources, something else will be impacted. These three indicators are therefore closely related, as security measures need to be undertaken based on their net benefit to the organisation, inefficiency of these measures needs to be quantified and used to set realistic expectations of the labour force. Even though existing literature mentions resource allocation and security budgeting as indicators for mature security governance [51, 2], almost no consideration is done about the inefficiency of security and expectations towards employees.

Conformance with internal and external requirements is already discussed in the previous section. Based on the research results 'compliance rate' was drafted as a performance indicator for security governance. The compliance rate is one of the most widely used indicators for security governance and adherence to the security policy [2, 51, 39, 48]. In consideration of the interview results, the focus group discussion and the papers by Beautement, Sasse, and Wonham [7], Fogg [26], and Sasse et al. [59], two additional subsets of the compliance rate were added to the performance indicator: effort and willingness of compliance (section 5.2, p.45-46).

Even though the rate of compliance of employees within an organisation gives some insight into whether employees are following the set policy, the underlying indicators of this compliance rate are even more important for governance. If the effort to comply with a security policy is too high, an employee might not comply anymore [7]. Also, the employee might still comply but starts to look for ways to undermine the organisation [7], which is not directly visible from the compliance rate. Alongside the effort to comply, the willingness to comply is equally relevant. As mentioned in section 5.2, compliance works best if employees are willing to do so [26, 59]. In order for this to work, the needs of the individual should be aligned with the business goals [59]. Currently, however, this does not seem to be entirely true. To illustrate this point, the closing paragraph of section 6.1.1 discussed how security measures were more costly against an arguably lower level of security. It is quite likely that this impacts the willingness of employees to comply. There is a wide variety of existing literature on compliance between an organisation and an employee on an individual level, but the results of the research have also shown that at Damen Naval there is a similar construction between an organisation and a client. During the group session, there were discussions on whether and how to comply with external regulations imposed by the client, which would indicate that compliance can be considered on multiple levels, inter- and intra- organisational. Inter-organisational, the performance indicator 'security governance vision' was drafted to compare potential misalignments in the internal vision and externally imposed requirements.

A final overarching security awareness indicator that is worth discussing further, is the ICT knowledge employees have. Multiple interviewees mentioned that for a security-conscious culture not only familiarity with the threat environment (indicator 10) is required, but also an understanding of ICT effects. This relates back to the introduction of the research (paragraph 1) which describes the impact of digitalization and the potential negative business impacts [5, 55]. It also mentions that 'the insider threat' needs to be considered and that this threat also comprises unintentional mistakes [14]. Results of the research indicate that not all employees understand the implications that digitalization brings forward and the potential consequences this has on security (subsection 5.1.5).

Apart from the overarching security governance performance indicators, a few indicators were drafted based on the research results from the individual security fields. Most of the indicators, at least the problems or issues that they were derived from have already been elaborated and do not need further discussion. However, one performance indicator that was assigned to access control, does require more thought. The indicator is the extent to which knowledge sharing is facilitated within the organisation of Damen Naval (indicator 5, subsection 5.2.2). In the literature review the trade-off in knowledge sharing vs. information protection was discussed. Elliott et al. [23] studied this trade-off in extensive detail. The paper mentions that depending on the classification of information and the extent to which client confidentiality is involved, security measures are often more strict [23]. Even though this aligns with the policy of Damen Naval, the interview results indicate that employees, especially engineers, would prefer to have more possibilities to share information. From a governance perspective, the trade-off with knowledge sharing is moving too much toward the protection of information and too little toward facilitating communication as well as physical gathering. A more mature security governance would therefore better align knowledge sharing with the protection of information.

6.1.3. Concordance

A special part of the research is related to reaching concordance. In the definition of mature security governance, the term concordance was used to describe the optimal way of alignment between security policies and business objectives. Concordance was defined as a negotiated treatment plan, with different parties taking on an active role in shaping a policy together [66, 4]. The lens with which the results were analysed was based on this shift from compliance to concordance (chapter 3). For this, the maturity of humans was used as a metaphor for relations within organisations (subsection 2.1.4), to understand how adults are expected to seek alignment and consensus more easily than infants as they become more conscientious, responsible and agreeable with age [58]. This parted from the views of Mettler, Rohner, and Winter [50] and Lasrado, Vatrapu, and Andersen [46] about something, i.e. the security policy, being complete, perfect or ready. Instead, this definition of maturity would suggest that the more willingness there is to engage in dialogue and to make a negotiated decision with the support of (representatives of) all parties involved, the more mature the security governance is. The metaphorical reference does not want to give the impression that organisations should just age in order to solve their problems. However, it does imply that organisations should act more socially mature. Imposing strict regulations and demanding compliance, without any input from other departments within the organisation would indicate a very low level of maturity and reaching concordance would indicate a very high level of maturity.

This being said, the results of the interviews as well as the focus group session indicate that, currently, no concordance is used in the alignment of business goals and security policies. It follows that the current security governance, based on the analysed security fields and the chosen dimensions, is not yet socially mature. Instead of an open discussion between adults, some dimensions of security governance would more relate to the quarrel between teenagers about what movie to go to. It would be unfair not to mention that there are aspects of the security governance at Damen Naval that have made strides from compliance to concordance. The security department is there to support the business, and, although it might not always be perceived that way, compliance is not merely enforced. Also, the security department aims to get involved with business and project meetings to put forward the perceptions and rationale behind certain policies. In these meetings, feedback on how policies should ideally be made is taken into account. From personal experience, the security department also hosted a project that aimed to inventory all the perceived security issues employees came across within projects. These issues were analysed and steps were considered to solve the issue or take away the perception of the security hindrance. On top of that, there can always be exceptions from regulations if the business determines this is worth it. Also, not all policies are strict and rule-based. Instead, in general, interviewees agreed that rules should be open to interpretation and that principle-based policies can be valuable for the empowerment of employees.

Despite the fact that Damen Naval is not currently actively adopting concordance in its security governance, the question remains whether this is at all possible for an organisation like Damen Naval, and if so, how concordance could be realised. The results indicate that concordance and the doctor-patient relationship are not directly translatable from the health sector to the naval shipbuilding sector. A doctor-patient relationship is, in principle, between two actors, whilst within Damen Naval up to 500 employees work on a single project. This multi-actor view on concordance brings forward additional levels of complexity as a negotiated treatment plan for each individual is not possible (section 5.3.4). Results do show that interviewees would propose a leading role of the business in policy-setting, instead of everything being 'governed' top-down. In the interviews, this was proposed to counter non-compliance, as engineers would find their own solutions with or without set policies (section 5.3.4, p.53-54). Despite the motivation behind it, this would be a good first step towards concordance. A more cumbersome finding of the discussion about concordance is that one of the interviewees related the doctor-patient to a mother-child relationship. Even though existing literature agrees that the expertise of the doctor should be used, the metaphor of a mother and child implies a significant imbalance in authority.

In order to make up for this imbalance, the group session agreed on a structure that was used at Damen Naval for project-related issues, in which working groups discuss issues with representatives of different departments/expertise on the same level of authority. A condition for reaching concordance is that relations should be on a similar field of authority. Within a hierarchical organisation such as Damen Naval, with different levels of authority (e.g., junior and senior engineers, subcontract managers, team leaders, project managers, board of directors, etc.) it is hard to reach concordance. Therefore, The group session proposed to work with two levels (working groups and steering committees), of which, on each respective level, a representation of the organisation discusses and decides how to approach an issue. The way this structure is implemented currently, decisions are still made top-down, based on the input of individuals.

I would argue, however, that it would be beneficial to let the working group discuss matters first and give their advice to the steering group. In this way, the structure follows a bottom-up approach and the working group does not merely have an execution role. Another issue with the current structure is that not every department is currently involved in the working group. Even though not all issues require the input of every department, one should be careful not to exclude departments beforehand. One of the key principles of concordance is that a treatment plan, i.e. a decision or policy is better supported if it is made with the input and expertise of all relevant stakeholders [66, 4]. This begs the question of who is a relevant stakeholder. Participants of the group session mentioned that there is no single list with representatives and that employees might be chosen case-specific. I would propose that all departments should at least be given transparency about the working groups on a lower level, with the opportunity to take part based on the appropriate argumentation. The available resources for each department should also be taken into account. Whereas engineering departments have multiple engineers for each subject, the security department has no direct counterparts. Even more so due to the differences in role and authority, as currently, security officers are communicating more on a management level. Therefore, it would be worthwhile to explore whether security-conscious engineers could represent the security department in lower-level working groups.

Even though not all aspects of the proposed structure are in line with the principles of concordance, overall it is considered to be a promising structure that can be tailored to work with security-related issues. Relating this back to the focus group session, the basic principles of inviting multiple employees with different views and expertise agree with the initial theory of what would be a good structure to align conflicts with security (policies) and productive work (contribution to business goals), as it corresponds with the conditions needed for reaching concordance. Also, based on the discussions of the security fields of access control and data classification, group session participants arguably were in more agreement after the session than before, as the discussions brought forward explanations of what data classification was used for. Despite no concrete solution approach (or treatment plan) being formulated, the participants had the opportunity of giving their viewpoints and some misconceptions were solved. The reason the group session was hosted the way it was, with representatives of different departments, already hints at what would be a suitable way of reaching concordance.

6.2. Reflection, limitations and future research

First, the methodological choices made were constrained by the time available for the thesis project, especially considering the ability to generalise the findings. Even though measures were taken to make the study more generalisable, such as applying the case study to specific security fields of the organisation, it would have been valuable to apply a similar case study to another organisation. Interestingly, many of the findings related to specific security fields, were generalisable to the organisation, which confirms that the results are at least generalisable to an organisational level. Considering the scope of the research and the extensive data gathered from the executed case study, the limitation has to be acknowledged but also accepted.

Related to this, the lack of interview data on external legislators limits the results in presenting any input from external organisations and therefore cannot confirm whether reaching concordance externally would be possible/worthwhile. However, the results have shown that external requirements were, in some instances, negatively impacting both security and productivity. Considering that external requirements such as the ABDO are put into place to ensure that security is aligned with the threat environment, one could at least imply that engaging in dialogue would contribute to the common good.

Future studies could look more into the effects of concordance on organisations bound by external requirements, as this study only briefly touched upon the external requirements and their implications for concordance. Future research could involve external organisations in the case study of the focal organisation. Applied to Damen Naval, this could be the ministry of Defense and the ABDO regulations. For other organisations or industries there might be other legislators. A condition for the research would be that there is an imbalance in authority. Instead of focusing on intra-organisational concordance, more research could thus be done on inter-organisational concordance.

A final aspect to note is the extent to which the results are operationalisable as the drafted performance indicators were not directly linked with an existing CMM framework. Despite the fact that a lot of CMM approaches were reviewed in the literature review and some aspects of those frameworks were used in the research, a comprehensive CMM framework for security governance that emphasizes the alignment of security policy with productivity, is yet to be found. During the initial stages of the thesis project the main goal of the thesis was to create such a framework. However, creating a maturity scale and at the same time being able to validate the levels of the scale was not feasible for a single case study within the projected time. After the kick-off meeting and consultation with my graduation committee, I decided to shift the research towards a framework for determining maturity. Even though the security governance indicators do not quantify or determine how mature security governance practices are, they do give direction on what aspects maturity needs to be addressed. This also enabled me to look more critically at the term 'maturity' and led me to introduce the concept of social maturity into the framework. The combination of conventional maturity and social maturity have not yet been used in governance frameworks, let alone in a CMM approach. Future work could build upon this research and develop a CMM framework for security governance that takes both of these interpretations of maturity for security governance into account.

7 Conclusion

This research aimed to build a framework for determining the maturity of security governance. The existing literature on mature security governance is not unanimous on how to approach security governance, let alone in determining the maturity. For this research, security governance is defined as the alignment between security policies and contribution to business goals, in which good governance operationalises into working both securely and productively. On top of that, mature security governance emphasises the alignment part of security and productivity, with the aim of reaching concordance, i.e. a negotiated policy among all representatives of the organisation, which is drafted in dialogue and with multi-actor expertise, instead of being mandated by a single actor (e.g. the security department). This parts from extant literature, about maturity being something that is 'perfect' or 'complete' in an absolute sense.

This being said the results of this study are two-fold: the framework has both a conventional assessment in terms of security governance performance, as well as an organisational and social aspect in terms of how alignment can best be reached. In the framework, this distinction is visualised by having both a conventional maturity side and a social maturity side. This research argues that both the conventional side of security governance and the social maturity part of security governance need to be considered in order to truly have mature security governance. An organisation that scores high on conventional maturity, e.g., by having clear organisation-wide role-setting, responsibility and ownership, might still lack social maturity. The research showed that the challenges and trade-offs employees perceive can not merely be solved by excelling in the conventional maturity of security governance. The way in which alignment between business goals and security policies is sought contributes to overall maturity. By means of a representative stakeholder dialogue on a balanced level of authority, a negotiated policy can be derived. This is different from having good top-down governance, as it involves representatives of the whole organisation and it acknowledges the department-specific challenges and expertise within the organisation.

The framework's foundation is built up of six dimensions along which the performance of security governance can be assessed, extracted from an extensive literature review. By means of a case study at Damen Naval in which the security dimensions were applied to interview questions, the security dimensions were operationalised into security governance performance indicators. Even though the case study was done on different security fields, most of the performance indicators are applicable to every security field, indicating that they are generalisable to the organisation. The most important indicators are about quantifying the inefficiency of security measures on productivity, as organisational decisions should follow based on the net benefit it delivers to the organisation. This also closely relates to the impact security measures have on the labour force and the expectations of (c-level) management towards employees. Another critical indicator is the compliance rate and the lower-level indicators of 'effort' and 'willingness', as these directly influence the compliance rate. The drafted security governance performance indicators may be used by Damen Naval, and potentially other organisations, in maturing their security governance. Each of the indicators steers on improving either or both security (in terms of policy-setting) and productivity (in terms of contribution to business goals).

The second part of the framework addresses social maturity, with the highest notion being to realise concordance with the security policy at Damen Naval. The final part of this study was to investigate whether concordance is possible within the context of an organisation such as Damen Naval and to discuss what it would take to reach such a state. The thesis has shown that engaging in dialogue with stakeholders about conflicts and trade-offs in security governance promotes alignment between productivity and security. Based on the conflicts and trade-offs that interviewees perceived related to security governance, a focus group session was hosted in which representatives of IT, the business and security could freely speak and discuss views. In a single session, this led to clarification about the use of data classification and access control, as well as an understanding of how strict the principles of need-to-know/be are currently set. This points to the conclusion that concordance is possible to a certain extent.

Nevertheless, in a big organisation with many stakeholders such as Damen Naval, reaching concordance is not particularly straightforward. Especially in comparison with the single-actor doctor-patient relationship in the healthcare industry. The research also acknowledged that 'true concordance' is paradoxical in organisations, as dialogue and stakeholder engagement should - at some point - be converged towards a policy that needs to be hierarchically imposed. Therefore, the framework has a back-and-forth relation between concordance and compliance. Furthermore, the strictly regulated environment wherein Damen Naval operates prohibits the organisation from maintaining full autonomy over its security policy. This also impacts how concordance can be realised, as it is dependent on multiple levels, both inter- and intra-organisational. To conclude, there is potential for concordance at Damen Naval, albeit in different forms and of increased complexity in comparison with the healthcare industry. Pained by the complexity of the industry and the playing field of different levels of concordance, a higher level of maturity of security governance will reap benefits for the organisation.

7.1. Recommendations for Damen Naval

In line with the extracted issues with security governance and the extracted performance indicators, the following recommendations are proposed for Damen Naval to address first:

1. Empower engineers into making an informed decision on data classification, but set the responsibility of classification to team leaders. Also, do not punish or impose negative consequences on engineers that made a - in hindsight - wrong informed decision on data classification, as this will cause engineers to classify documents unnecessarily high (subsection 5.1.1 'Shared responsibility or lack of ownership' and subsection 5.1.4 'Classification: black and white or grey?').
2. Put more emphasis on quantifying the costs and the benefits of security measures. This would, if done correctly, explain to employees why certain measures are taken (thereby promoting the willingness of employees to comply), or if there is no net benefit, give the incentive to change the policy (subsection 5.1.3).

3. In line with the previous point, for externally imposed requirements that have no net benefit for the organisation, engage in dialogue with the client if these measures are there for the common good or if something can be done to improve (subsection 5.1.4).
4. Be transparent and clear in expectations towards employees. Do not let employees absorb the additional hours it would take them to do productive work, due to security measures. This will result in a negative impact, either in non-compliance to security measures, quality of work or personal strain when the former two aspects are not impacted (subsection 5.1.4 and point 7 of the performance indicators).
5. Promote knowledge sharing by clarifying the need-to-know principle to include the 'need' for engineers to learn from colleagues of different disciplines, instead of restricting access to information that is not directly necessary for the primary function of an individual (subsection 5.1.4).
6. Improve (security) awareness among engineers. Not only does this comprise the understanding of security policies and familiarity with the threat environment of Damen Naval. It should also include awareness of the prominent role ICT solutions play in day-to-day activities and the potential (negative) consequences this might have on security (subsection 5.1.5).

Finally, an organisational structure is advised that facilitates concordance both inter- and intra-organisational (addressed in subsection 5.3.4). Within the organisation, the concordance structure of working groups and steering committees is recommended. This structure could either be implemented into existing working groups of the business or a new structure could be set up. Implementation into existing working groups and steering committees has the advantage that only minor changes need to be done to the organisation. Also, no new meetings have to be scheduled, as the inclusion of security-related topics can be adopted in the same meeting as other issues. A potential disadvantage is that the security department would be unable to join all lower-level working group meetings. This could be resolved by enabling a particular security-conscious project engineer to represent the security department on a lower level and only including the security department if escalation is required. An advantage of setting up a new structure is that the alignment between security and productivity can play a more prominent role, as this will be the starting point of the meeting.

Externally, dialogue with clients and external regulators should be pursued. A lobbying group for regulation change of the ABDO is currently active (section 5.1.4). The same way concordance can be achieved internally, Damen Naval could propose a meeting with stakeholders impacted by the ABDO requirements. A premise of being able to pursue concordance is to use the drafted security governance framework. This will enable Damen Naval to determine the impact of security measures on security and business goals. This way, Damen Naval can demonstrate whether or not the regulations of the client and regulator are worth changing. Similarly, other involved stakeholders that are impacted by the regulations, can measure the impact on security governance in a similar fashion. If most of the stakeholders involved are negatively impacted by the same regulations, a larger support base can be formed for convincing the regulator into changing the regulations.

If, on the other hand, there is no united front for changing a regulation, at least all the stakeholders involved are able to discuss based on a comprehensive way of security governance, that acknowledges that security governance is more than the isolated policies of an organisation.

References

[1] Richard M. Adler. “A dynamic capability maturity model for improving cyber security”. In: *2013 IEEE International Conference on Technologies for Homeland Security (HST)*. 2013 IEEE International Conference on Technologies for Homeland Security (HST). Nov. 2013, pp. 230–235. DOI: 10.1109/THS.2013.6699005.

[2] Sultan AlGhamdi, Khin Than Win, and Elena Vlahu-Gjorgievska. “Information security governance challenges and critical success factors: Systematic review”. In: *Computers & Security* 99 (Dec. 1, 2020), p. 102030. ISSN: 0167-4048. DOI: 10.1016/j.cose.2020.102030. URL: https://www.sciencedirect.com/science/article/pii/S0167404820303035 (visited on 03/27/2023).

[3] Ross Anderson and Tyler Moore. “The Economics of Information Security”. In: *Science* 314.5799 (Oct. 27, 2006). Publisher: American Association for the Advancement of Science, pp. 610–613. DOI: 10.1126/science.1130992. URL: https://www.science.org/doi/10.1126/science.1130992 (visited on 03/29/2023).

[4] Debi Ashenden, Gail Ollis, and Iain Reid. “Dancing, not Wrestling: Moving from Compliance to Concordance for Secure Software Development”. In: *37th IEEE/ACM International Conference on Automated Software Engineering*. ASE ’22: 37th IEEE/ACM International Conference on Automated Software Engineering. Rochester MI USA: ACM, Oct. 10, 2022, pp. 1–9. ISBN: 978-1-4503-9475-8. DOI: 10.1145/3551349.3561145. URL: https://dl.acm.org/doi/10.1145/3551349.3561145 (visited on 03/14/2023).

[5] Syahirah Azizan et al. “Exploring The Factors That Influence The Success Of Digitalization In An Organization’s IT Department”. In: *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*. 2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE). Vol. 6. Dec. 2021, pp. 1–6. DOI: 10.1109/ICRAIE52900.2021.9704018.

[6] Corlane Barclay. “Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model (CM2)”. In: *Proceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world - Impossible without standards?* Proceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world - Impossible without standards? June 2014, pp. 275–282. DOI: 10.1109/Kaleidoscope.2014.6858466.

[7] Adam Beautement, Angela Sasse, and Mike Wonham. “The compliance budget: managing security behaviour in organisations”. In: (Sept. 22, 2008). DOI: 10.1145/1595676.1595684.

[8] Bojarow. *Reddit - Dive into anything*. 2020. URL: https://www.reddit.com/r/WarshipPorn/comments/jwftrf/a_look_from_above_at_the_f_126_frigate_the/.

[9] Rossouw de Bruin and S. H. von Solms. “Modelling Cyber Security Governance Maturity”. In: *2015 IEEE International Symposium on Technology and Society (ISTAS)*. 2015 IEEE International Symposium on Technology and Society (ISTAS). ISSN: 2158-3412. Nov. 2015, pp. 1–8. DOI: 10.1109/ISTAS.2015.7439415.

[10] F. Buytendijk and B. Willemsen. *How to Manage Digital Ethical Dilemmas*. Gartner. Dec. 15, 2022. URL: https://www.gartner.com/document/4022267?ref=solrResearch&refval=364171149 (visited on 04/19/2023).

[11] Mariana G. Cains et al. "Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation". In: *Risk Analysis* 42.8 (2022). _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/risa.13687, pp. 1643–1669. ISSN: 1539-6924. DOI: 10.1111/risa.13687. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.13687 (visited on 03/01/2023).

[12] Antonio José Carpio-de los Pinos et al. "Zero-Risk Interpretation in the Level of Preventive Action Method Implementation for Health and Safety in Construction Sites". In: *International Journal of Environmental Research and Public Health* 18.7 (Mar. 29, 2021), p. 3534. ISSN: 1661-7827. DOI: 10.3390/ijerph18073534. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8038139/ (visited on 03/01/2023).

[13] Cisco. *What Is Cybersecurity?* Oct. 2022. URL: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

[14] Carl Colwill. "Human factors in information security: The insider threat – Who can you trust these days?" In: *Information Security Technical Report* 14.4 (2009). Human Factors in Information Security, pp. 186–196. ISSN: 1363-4127. DOI: https://doi.org/10.1016/j.istr.2010.04.004. URL: https://www.sciencedirect.com/science/article/pii/S1363412710000051.

[15] Corallo, Lazoi, and Lezzi. "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts". In: *Computers in Industry* 114.103165 (Dec. 2017). DOI: 10.1109/ICCAD.2017.8203896. URL: https://www-sciencedirect-com.tudelft.idm.oclc.org/science/article/pii/S0166361519304427.

[16] James Crotty and Elizabeth Daniel. "Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment". In: *Applied Computing and Informatics* ahead-of-print (ahead-of-print Jan. 1, 2022). ISSN: 2210-8327. DOI: 10.1108/ACI-07-2022-0178. URL: https://doi.org/10.1108/ACI-07-2022-0178 (visited on 02/13/2023).

[17] D-Mitch. *INFOGRAPHICS 58: Future Surface Combatants Vol. III (Arrowhead 140PL, Thaon di Revel-class, F126-class)*. Aug. 2022. URL: https://www.navalanalyses.com/2022/08/infographics-58-future-surface.html.

[18] Damen Schelde Naval Shipyards. *BUSINESS PLAN 2021 - 2025: Division Naval*. Num Pages: 27. Sept. 4, 2020. (Visited on 04/05/2023).

[19] Rossouw De Bruin and S. H. von Solms. "Cybersecurity Governance: How can we measure it?" In: *2016 IST-Africa Week Conference*. 2016 IST-Africa Week Conference. May 2016, pp. 1–9. DOI: 10.1109/ISTAFRICA.2016.7530578.

[20] Dictionary. "Definition of alignment". In: URL: https://www.dictionary.com/browse/alignment.

[21] Cambridge Dictionary. "security definition: 1. protection of a person, building, organization, or country against threats such as crime or…. Learn more." In: Feb. 2023. URL: https://dictionary.cambridge.org/dictionary/english/security.

[22] Durga Prasad Dube and R. P. Mohanty. "Towards development of a cyber security capability maturity model". In: *International Journal of Business Information Systems* (Apr. 16, 2020). Publisher: Inderscience Publishers (IEL). URL: https://www.inderscienceonline.com/doi/10.1504/IJBIS.2020.106800 (visited on 03/10/2023).

[23] Karen Elliott et al. “Knowledge Protection in Firms: A Conceptual Framework and Evidence from HP Labs”. In: *European Management Review* 16.1 (2019), pp. 179–193. ISSN: 1740-4762. DOI: 10.1111/emre.12336. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/emre.12336 (visited on 03/15/2023).

[24] U.S. Department of Energy. *Cybersecurity Capability Maturity Model (C2M2)*. Tech. rep. June 2022. URL: https://www.energy.gov/sites/default/files/202206/C2M2%20Version%202.1%20June%202022.pdf.

[25] Beyzanur Cayir Ervural and Bilal Ervural. “Overview of Cyber Security in the Industry 4.0 Era”. In: *Industry 4.0: Managing The Digital Transformation*. Cham: Springer International Publishing, 2018, pp. 267–284. ISBN: 978-3-319-57870-5. DOI: 10.1007/978-3-319-57870-5_16. URL: https://doi.org/10.1007/978-3-319-57870-5_16.

[26] Bj Fogg. “A behavior model for persuasive design”. In: *Proceedings of the 4th International Conference on Persuasive Technology*. Persuasive 2009: Persuasive 2009; 4th International Conference on Persuasive Technology. Claremont California USA: ACM, Apr. 26, 2009, pp. 1–7. ISBN: 978-1-60558-376-1. DOI: 10.1145/1541948.1541999. URL: https://dl.acm.org/doi/10.1145/1541948.1541999 (visited on 06/08/2023).

[27] Peter Gal et al. “Digitalization and productivity: in search of the holy grail-firm-level empirical evidence from European countries”. In: *International Productivity Monitor* 37.Fall (2019), pp. 39–71.

[28] “Gartner Identifies 3 Factors Influencing Growth in Security Spending”. In: (Oct. 2022). URL: https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i.

[29] Ghada Gashgari, Robert Walters, and Gary Wills. “A Proposed Best-practice Framework for Information Security Governance:” in: *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*. 2nd International Conference on Internet of Things, Big Data and Security. Porto, Portugal: SCITEPRESS - Science and Technology Publications, 2017, pp. 295–301. ISBN: 978-989-758-245-5. DOI: 10.5220/0006303102950301. URL: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0006303102950301 (visited on 04/05/2023).

[30] Damen Shipyards Group. *About Damen Shipyards | Damen*. URL: https://www.damen.com/about.

[31] Florian Guggenmos et al. “Security First, Security by Design, or Security Pragmatism – Strategic Roles of IT Security in Digitalization Projects”. In: *Computers & Security* 118 (July 1, 2022), p. 102747. ISSN: 0167-4048. DOI: 10.1016/j.cose.2022.102747. URL: https://www.sciencedirect.com/science/article/pii/S0167404822001420 (visited on 02/14/2023).

[32] R. Gulzar and J. Kopcho. *5 Key Changes to Achieve Just-Enough IT Governance*. Gartner. July 12, 2022. URL: https://www.gartner.com/document/4016466?ref=solrResearch&refval=364165293 (visited on 04/19/2023).

[33] Zelee Hill et al. “Are verbatim transcripts necessary in applied qualitative research: experiences from two community-based intervention trials in Ghana”. In: *Emerging Themes in Epidemiology* 19.1 (Dec. 2022). Number: 1 Publisher: BioMed Central, pp. 1–8. ISSN: 1742-7622. DOI: 10.1186/s12982-022-00115-w. URL: https://ete-online.biomedcentral.com/articles/10.1186/s12982-022-00115-w (visited on 05/18/2023).

[34] Erik Hollnagel. “The ETTO Principle - Efficiency-Thoroughness Trade-Off”. In: (May 2009). URL: https://erikhollnagel.com/onewebmedia/ETTO.pdf.

[35] Val Hooper and Jeremy McKissack. “The emerging role of the CISO”. In: *Business Horizons* 59.6 (2016). CYBERSECURITY IN 2016: PEOPLE, TECHNOLOGY, AND PROCESSES, pp. 585–591. ISSN: 0007-6813. DOI: https://doi.org/10.1016/j.bushor.2016.07.004. URL: https://www.sciencedirect.com/science/article/pii/S0007681316300635.

[36] Transforma Insights. *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030 (in billions) [Graph]*. July 2022. URL: https://www-statista-com.tudelft.idm.oclc.org/statistics/1183457/iot-connected-devices-worldwide/.

[37] ISACA. *COBIT 5 for Information Security*. Google-Books-ID: XSuFnQEACAAJ. ISACA, 2012. 220 pp. ISBN: 978-1-60420-254-0.

[38] ISACA. *INTRODUCING OVERVIEW COBIT 2019*. Tech. rep. Nov. 2018. URL: https://www.isaca.org/resources/cobit.

[39] ISO/IEC. *NEN Connect - NEN-ISO/IEC 27014:2020 en*. 2020. URL: https://connect.nen.nl/Standard/Detail/3641071?compId=10037&collectionId=0.

[40] David James and Canesio Predo. “Principles and Practice of Cost–Benefit Analysis”. In: *Cost-Benefit Studies of Natural Resource Management in Southeast Asia*. Ed. by David James and Herminia A. Francisco. Singapore: Springer, 2015, pp. 11–46. ISBN: 978-981-287-393-4. DOI: 10.1007/978-981-287-393-4_2. URL: https://doi.org/10.1007/978-981-287-393-4_2 (visited on 06/21/2023).

[41] Allan Jay. *How many IoT connected devices were installed in 2020? The number of connected Internet of Things (IoT) device*. Jan. 2023. URL: https://financesonline.com/number-of-internet-of-things-connected-devices/.

[42] Val Hooper anMarian Carcaryd Tarika Kalidas. “IT Risk Management: A Capability Maturity Model Perspective”. In: *Electronic Journal of Information Systems Evaluation* 16.1 (June 1, 2013). Number: 1, pp3□13–pp3□13. ISSN: 1566-6379. URL: https://academic-publishing.org/index.php/ejise/article/view/217 (visited on 03/10/2023).

[43] Kunwoo Kim and Jungduk Kim. “A Role of Information Security Committee based on Competing Values Framework”. In: *Proceedings of the 17th International Conference on Electronic Commerce 2015*. ICEC ’15: The 17th International Conference on Electronic Commerce 2015. Seoul Republic of Korea: ACM, Aug. 3, 2015, pp. 1–4. ISBN: 978-1-4503-3461-7. DOI: 10.1145/2781562.2781600. URL: https://dl.acm.org/doi/10.1145/2781562.2781600 (visited on 03/27/2023).

[44] Iacovos Kirlappos, Adam Beautement, and M. Angela Sasse. ““Comply or Die” Is Dead: Long Live Security-Aware Principal Agents”. In: *Financial Cryptography and Data Security*. Ed. by Andrew A. Adams, Michael Brenner, and Matthew Smith. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2013, pp. 70–82. ISBN: 978-3-642-41320-9. DOI: 10.1007/978-3-642-41320-9_5.

[45] Kost. *Engaging the Right People Is the Most Critical Success Factor of Government Governance*. Gartner. Apr. 12, 2023. URL: https://www.gartner.com/document/4265199 (visited on 04/19/2023).

[46] Lester Lasrado, Ravi Vatrapu, and Kim Normann Andersen. *MATURITY MODELS DEVELOPMENT IN IS RESEARCH: A LITERATURE REVIEW*. Aug. 9, 2015. DOI: 10.13140/RG.2.1.3046.3209.

[47] Julie A. Luft et al. “Literature Reviews, Theoretical Frameworks, and Conceptual Frameworks: An Introduction for New Biology Education Researchers”. In: *CBE- Life Sciences Education* 21.3 (Sept. 2022). DOI: 10.1187/cbe.21-05-0134. URL: https://doi.org/10.1187/cbe.21-05-0134.

[48] Yassine Maleh et al. “A Capability Maturity Framework for IT Security Governance in Organizations”. In: *Innovations in Bio-Inspired Computing and Applications*. Ed. by Ajith Abraham et al. Advances in Intelligent Systems and Computing. Cham: Springer International Publishing, 2018, pp. 221–233. ISBN: 978-3-319-76354-5. DOI: 10.1007/978-3-319-76354-5_20.

[49] Incorporated Merriam-Webster. “Definition of governance”. In: Mar. 2023. URL: https://www.merriam-webster.com/dictionary/governance.

[50] Tobias Mettler, Peter Rohner, and Robert Winter. “Towards a Classification of Maturity Models in Information Systems”. In: *Management of the Interconnected World*. Ed. by Alessandro D’Atri et al. Heidelberg: Physica-Verlag HD, 2010, pp. 333–340. ISBN: 978-3-7908-2404-9. DOI: 10.1007/978-3-7908-2404-9_39.

[51] Sushma Mishra. “Organizational objectives for information security governance: a value focused assessment”. In: *Information & Computer Security* 23.2 (Jan. 1, 2015). Publisher: Emerald Group Publishing Limited, pp. 122–144. ISSN: 2056-4961. DOI: 10.1108/ICS-02-2014-0016. URL: https://doi.org/10.1108/ICS-02-2014-0016 (visited on 03/31/2023).

[52] Valentin Mullet, Patrick Sondi, and Eric Ramat. “A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0”. In: *IEEE Access* 9 (2021). Conference Name: IEEE Access, pp. 23235–23263. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3056650.

[53] Simon Parkin et al. “A Stealth Approach to Usable Security: Helping IT Security Managers to Identify Workable Security Solutions”. In: *Proceedings of the 2010 New Security Paradigms Workshop*. NSPW ’10. Concord, Massachusetts, USA: Association for Computing Machinery, 2010, pp. 33–50. ISBN: 9781450304153. DOI: 10.1145/1900546.1900553. URL: https://doi-org.tudelft.idm.oclc.org/10.1145/1900546.1900553.

[54] Mark C. Paulk. “A History of the Capability Maturity Model for Software”. In: *Software Quality Professional Magazine* 12 (Dec. 2009). URL: http://asq.org/software-quality/2009/12/process-management/a-history-of-the-capability-maturity-model-for-software.pdf.

[55] Jaco Prinsloo, Saurabh Sinha, and Basie von Solms. “A Review of Industry 4.0 Manufacturing Process Security Risks”. In: *Applied Sciences* 9.23 (2019). ISSN: 2076-3417. DOI: 10.3390/app9235105. URL: https://www.mdpi.com/2076-3417/9/23/5105.

[56] Ganesh B. Regulwar, V.S. Gulhane, and P. M. Jawandhiya. “A Security Engineering Capability Maturity Model”. In: *2010 International Conference on Educational and Information Technology*. 2010 International Conference on Educational and Information Technology. Vol. 1. Sept. 2010, pp. V1–306–V1–311. DOI: 10.1109/ICEIT.2010.5607700.

[57] D. Reinsel, J. Gantz, and J. Rydning. *The Digitization of the World From Edge to Core*. Tech. rep. Nov. 2018. URL: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

[58] Brent W. Roberts and Daniel Mroczek. “Personality Trait Change in Adulthood”. In: *Current directions in psychological science* 17.1 (Feb. 1, 2008), pp. 31–35. ISSN: 0963-7214. DOI: 10.1111/j.1467-8721.2008.00543.x. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2743415/ (visited on 03/15/2023).

[59] M. Angela Sasse et al. “Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours”. In: *Computer Security. ESORICS 2022 International Workshops*. Ed. by Sokratis Katsikas et al. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2023, pp. 248–265. ISBN: 978-3-031-25460-4. DOI: 10.1007/978-3-031-25460-4_14.

[60] Stef Schinagl and Abbas Shahim. “What do we know about information security governance? “From the basement to the boardroom”: towards digital security governance”. In: *Information & Computer Security* 28.2 (Jan. 1, 2020). Publisher: Emerald Publishing Limited, pp. 261–292. ISSN: 2056-4961. DOI: 10.1108/ICS-02-2019-0033. URL: https://doi.org/10.1108/ICS-02-2019-0033 (visited on 03/27/2023).

[61] “security”. In: Feb. 2023. URL: https://www.merriam-webster.com/dictionary/security.

[62] Uma Sekaran and Roger Bougie. *Research Methods For Business*. Hoboken, NJ, United States: Wiley, 2020.

[63] Damen Schelde Naval Shipbuilding. *Integraal beveiligingsplan*. Tech. rep. QK0030.10. Version 3. Feb. 2022.

[64] G. Terry et al. *Thematic Analysis*. SAGE, 2017. URL: https://books.google.nl/books?hl=nl&lr=&id=AAniDgAAQBAJ&oi=fnd&pg=PA17&dq=thematic+analysis+braun+and+clarke&ots=doo5mlDkH-&sig=FtGtEDp_enFPbmnRDWEe_j7iA28#v=onepage&q=thematic%20analysis%20braun%20and%20clarke&f=false.

[65] Cristian Vartolomei and Silvia Avasilcăi. “Security and Privacy Implementation Framework as a Result of the Digitalization Process for Organizations in Different Industries”. In: Cited by: 0. 2020, pp. 41–51. DOI: 10.1007/978-3-030-44711-3_4. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85126134298&doi=10.1007%2f978-3-030-44711-3_4&partnerID=40&md5=c07fc4e7e3fcf8350f656fb6d5b5f247.

[66] E. Vermeire et al. “Patient adherence to treatment: three decades of research. A comprehensive review”. In: *Journal of Clinical Pharmacy and Therapeutics* 26.5 (2001). _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1046/j.1365-2710.2001.00363.x, pp. 331–342. ISSN: 1365-2710. DOI: 10.1046/j.1365-2710.2001.00363.x. URL: https://onlinelibrary.wiley.com/doi/abs/10.1046/j.1365-2710.2001.00363.x (visited on 05/01/2023).

[67] Bernard Vrijens et al. “A new taxonomy for describing and defining adherence to medications”. In: *British Journal of Clinical Pharmacology* 73.5 (2012), pp. 691–705. ISSN: 1365-2125. DOI: 10.1111/j.1365-2125.2012.04167.x. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1365-2125.2012.04167.x (visited on 05/01/2023).

[68] J. R. Westby and J. H. Allen. *Governing for Enterprise Security (GES) Implementation Guide.* ADA472572. Num Pages: 116. Carnegie-Mellon Univ., Pittsburgh, PA. Software Engineering Inst., 2007. URL: https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA472572.xhtml (visited on 04/05/2023).

[69] Patricia Williams. “A practical application of CMM to medical security capability”. In: *Information Management & Computer Security* 16.1 (Jan. 1, 2008). Publisher: Emerald Group Publishing Limited, pp. 58–73. ISSN: 0968-5227. DOI: 10.1108/09685220810862751. URL: https://doi.org/10.1108/09685220810862751 (visited on 02/23/2023).

[70] Steven Woodhouse. “An ISMS (Im)-Maturity Capability Model”. In: *2008 IEEE 8th International Conference on Computer and Information Technology Workshops*. 2008 IEEE 8th International Conference on Computer and Information Technology Workshops. July 2008, pp. 242–247. DOI: 10.1109/CIT.2008.Workshops.46.

[71] Robert K. Yin. *Case study research: design and methods*. 4th ed. Applied social research methods v. 5. Los Angeles, Calif: Sage Publications, 2009. 219 pp. ISBN: 978-1-4129-6099-1.

[72] Tanveer A. Zia. “Organisations Capability and Aptitude towards IT Security Governance”. In: *2015 5th International Conference on IT Convergence and Security (ICITCS)*. 2015 5th International Conference on IT Convergence and Security (ICITCS). Aug. 2015, pp. 1–4. DOI: 10.1109/ICITCS.2015.7293005.

[73] E. Zio. “The future of risk assessment”. In: *Reliability Engineering System Safety* 177 (2018), pp. 176–190. ISSN: 0951-8320. DOI: https://doi.org/10.1016/j.ress.2018.04.020. URL: https://www.sciencedirect.com/science/article/pii/S0951832017306543.

A
Overview interview questions

Table A.1: Introductory and overarching interviewee questions

Interview question	**Goal**	**Security governance dimension**
What is your role at Damen Naval and what activities does your usual day involve?	General idea about the role of the interviewee and his/her expertise	-
What do you believe would be the business objectives of Damen Naval? (and the objectives in your role?)	If security governance is about alignment between security policy and business objectives, the perceptions of employees on the latter need to be taken into account	-
What do you consider to be your role in [security field], if any?	Insight into the involvement of employee in [security field] and in perspective to theoretical roles (policy)	Organisation-wide security and responsibility/accountability
Do you know where to find the right procedures for [security field], and if so, are they clear to you?	Understanding whether employees need and use procedures for their work or if this is within the capability of the employee	Security positive/conscious culture
What dilemmas or trade-offs would a fictional colleague encounter regarding compliance to [security field], if any?	Finding dilemmas and possibly workarounds for how employees deal with security restrictions	Conformance with internal and external requirements, Risk-based approach, Security positive/conscious culture
Would you say that the security policy of [security field] is aligned with business objectives and project goals?	Performance measure for security governance, with possible explanation of security governance issues	Security performance measurement /alignment

Table A.2: Specific interview questions on access control

Interview question	**Goal**	**Security governance dimension**
Is knowledge sharing at Damen Naval encouraged?	Knowledge sharing may be restricted due to the restrictions in access to files/folders, etc. This question aims to get an understanding of how knowledge is being shared as well as to investigate the trade-off in securing information and sharing information [23].	Risk-based approach, Conformance with internal and external requirements, security performance measurement/alignment
Would you prefer an optimistic security policy relating to access control, i.e. the starting point being that employees have access, unless enforcement is needed, over a conventional 'no-access' unless .. policy?	Perception of different employees on trade-off between security and accessibility	Security positive/conscious culture, Direction of acquisition and commitment of resources, Risk-based approach
Fill in	Fill in	Fill in

Table A.3: Specific interview questions on Data classification

Interview question	**Goal**	**Security governance dimension**
On what grounds would you say that data is classified?	Basic understanding of how employees perceive data classification and how they classify data	Risk-based approach, Conformance with internal and external requirements, security positive/conscious culture, security performance measurement/alignment
Would you say that, generally, information is classified correctly (level of confidentiality mentions classification)?	Performance measure and indicator for whether classification is done accordingly	Conformance with internal and external requirements, Security performance measurement/alignment
To your best knowledge, what would be the consequence of classifying a document too low? And too high?	Understanding of the potential consequences of classifying information wrong as well as who is impacted by this.	Security positive/conscious culture, Risk-based approach, conformance with internal and external requirements
Who / what department is responsible for data classification?	Understanding about how interviewees see the responsibility structure for access control compared to the policy.	Organisation-wide security and responsibility/accountability, conformance with internal and external requirements

Table A.4: Specific interview questions on Monitoring & Incident response

Interview question	Goal	Security governance dimension
Would you be able to define the threat landscape Damen Naval is operating in?	Indication of the threat awareness of employees and specific industry that Damen Naval is operating within	Risk-based approach, security positive/conscious culture, Organisation-wide security and responsibility/accountability
Is the incident management process regularly updated or is the process flow itself stable/static?	Performance measure and indicator for the way the policy of incident response is shaped	Security performance measurement/alignment
Are you aware of the target response times and target resolution times that are included in the incident management process, and, if so, are they feasible?	Understanding whether employees are aware of the response times and if they benchmark their response to this.	Conformance with internal and external requirements, Security performance measurement/alignment
In an ideal world, how would monitoring & incident response governance at Damen Naval look like?	Perception of employees and their vision on what would be a good structure for monitoring & incident response. Also makes comparison with the current situation possible.	Security performance measurement/alignment, conformance with internal and external requirements, Direction of acquisition and commitment of resources