A Cybersecurity Supervision Model for the Dutch Military Domain

Rijk, Eric de

Executive Master Cyber Security

Faculty of Governance and Global Affairs

A Cybersecurity Supervision Model for the Dutch Military Domain

Name:	Eric de Rijk
Student-no:	S2005271
Date:	28-2-2024
1st supervisor:	Jan van den Berg
2nd supervisor:	Tommy van Steen

Management Summary

Innovative civilian technologies are expected to provide many new opportunities in many sectors or "*verticals*," such as finance, transportation, healthcare, and the military. Moreover, information-driven tactical decision-making Information- and Operational Technology (IT/OT) supporting, for example, weapon systems are considered critical for the Dutch military fighting power.
Through step-by-step innovation programs, the Dutch military's *"digital transformation"* to an integrated Service Oriented Architecture (SOA) has started and will continue for many years to come. However, participating in cyberspace is not without security risks. These cybersecurity risks may backfire and challenge the Dutch military's expected advantage over the enemy.
The digital threat to the Netherlands remains unabatedly high and changes constantly, according to the '*Cyber Security Assessment Netherlands 2023*'. Because IT increasingly supports vital processes of the Dutch military and its partners in the public and private sectors, and cybersecurity risks also increase, it is no surprise that Dutch military and (inter)national cybersecurity regulations are also becoming stricter. Furthermore, cybersecurity governance and especially supervision are of the utmost importance for the Dutch military and society to place trust in IT services. Trust is a necessary condition for releasing the expected benefits. [1] It concerns the security of every aspect of IT services, ranging from compliance management and decision-making, human behavior and confidentiality, integrity, and availability of data and services. From a governance perspective, it implies end-to-end security for the Dutch military and society.
This thesis examines corporate governance and, more specifically, cybersecurity supervision challenges within the Dutch military domain's rapidly changing digital environment. Within this view, managing existing and newly upcoming risks by Dutch military operational and supporting units requires an integral supervision approach. The overall objective is to design an integrated approach for supervisors to ensure cybersecurity trust with Dutch military stakeholders.

Corporate governance involves establishing regulations and continuous monitoring of their proper implementation by the Board of Directors (BOD). The executive BOD directors, responsible for managing IT services at the strategic level, must deal with threats from the growing attack surface. Executive directors are expected to account to the non-executive BOD directors (independent supervisors) for the feasibility of the principles of long-term value creation versus risk and compliance management. [2]
The Dutch military governance directive "Governance of Defence" aligns precisely with the governance layer of the 3-layer *cyberspace conceptualization* by Van den Berg et al. [3] and the governance principles for value creation, risk management, and supervision.
Based on the statements from the Ministry of the Interior and Kingdom Relations, [4] the Scientific Council for Government Policy, [5] the Dutch Cabinet instructions, [6] the Dutch monitoring committee, [2] and the Dutch Inspection Council, [7] the objectives for cybersecurity supervision for gaining mutual trust in IT platform services by its actors and society are: (1) applying a risk-based approach executed by (2) cooperating supervisory bodies based on (3) cybersecurity controls for (4) compliance monitoring, and (5) intervention (in the event of non-compliance).

Generally, the (inter)national law aims to prevent and mitigate security breaches and contains a *duty of care* that obliges regulated entities to carry out a risk assessment. Other objectives are to oblige regulated entities for incident reporting, introduce a more intensive supervision regime, and contribute to more significant harmonization and a higher level of cyber security in organizations.
The Dutch military (cyber) security regulations stem from the decree Chief Security Officer (CSO) structure civil service (2021) and NATO. An essential supervision objective of the civil service decree and NATO regulations is the formal approval to use IT platform services for special information processing "*to ensure an appropriate level of security given the interest to be protected*."

Following the Hevner et al. design science methodology [8] and based on the identified challenges for meeting its five cybersecurity supervision objectives, the succeeding design requirements for corporate cybersecurity supervision became apparent:

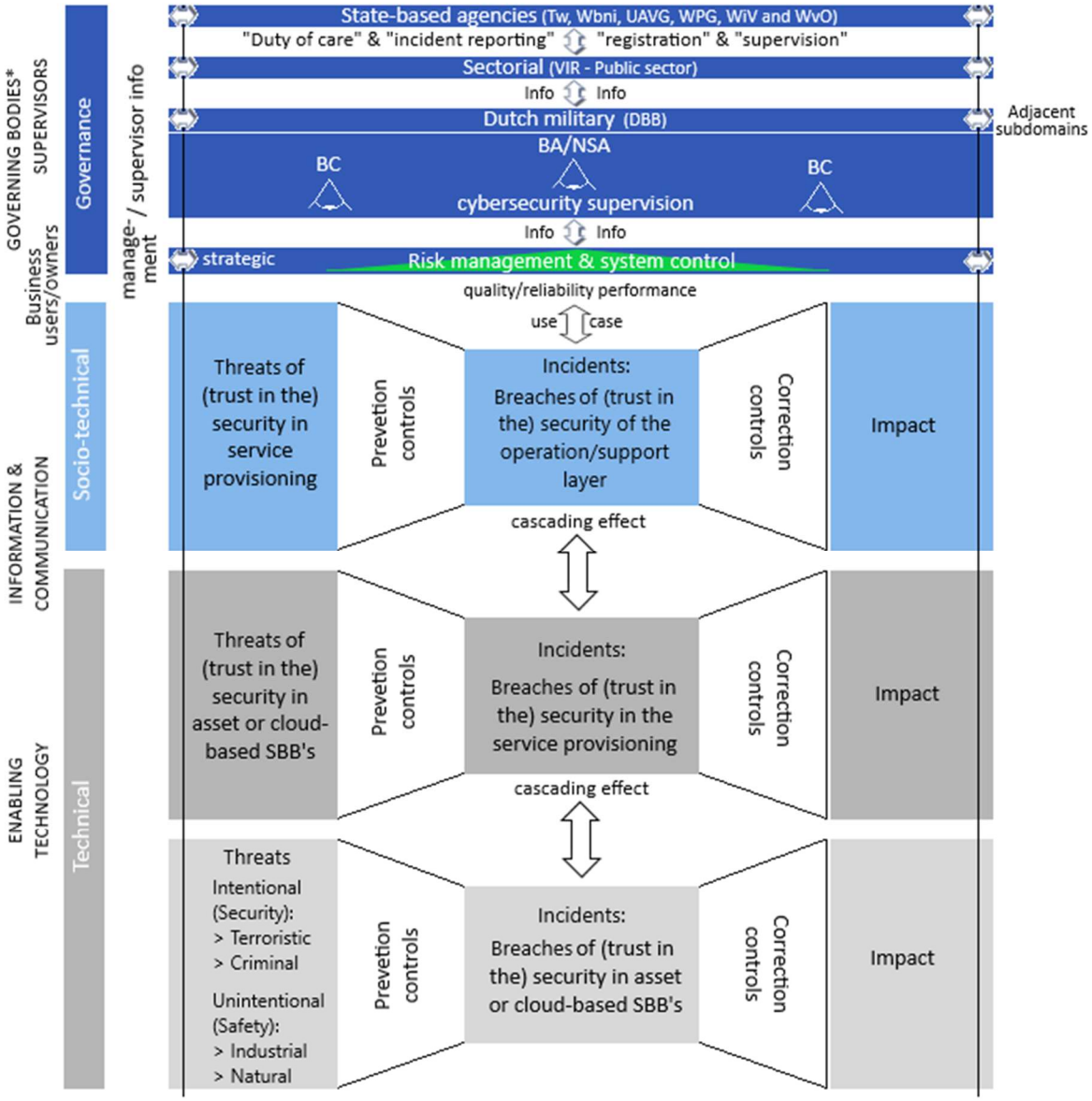
1. Implement a risk-based approach considering cascading effects into adjacent subdomains that support Dutch military and partner units;
2. Cooperation between supervisors of adjacent subdomains that support Dutch military and partner units;
3. Application of mutually accepted and up-to-date cybersecurity control frameworks;
4. Collect information from supervisors from the growing number of Dutch military and partner units to create situational awareness. Units with, for example, IT service contractors and sub-contractors. Supervisors address this by focusing on the effective operation of a risk management and control system and their mutual coordination in monitoring compliance. Therefore, supervisors must focus on systemic risks (and some "*random security tests*[1]*"*) instead of time-consuming low-level risks (treatment of symptoms);
5. Intervene in the event of non-compliance, considering systemic risks (with cascading effects) and using up-to-date controls accepted by supervisors for adjacent subdomains supporting the diverse Dutch military and partner units.

The first design requirement for an integrated cybersecurity supervision model for the Dutch military domain is implementing a risk-based supervision approach considering cascading effects into adjacent subdomains that support Dutch military and partner units.

Following the *cyberspace conceptualization*, the provisioning of IT (platform) services is modeled in the Dutch military supervision, owner, operation/support, provider, and Service Building Block (SBB) layers. After that, the "Bowtie" methodology (identifying, assessing, analyzing, and handling risks) models the risks arising from breaches of (trust in the) security in the (multi-stakeholder) IT platform services.
The "*Bowtie*" methodology illustrates the relationship between threats, prevention controls, (inter)dependent incidents, repression controls, and impact (risks).
Combining the provisioning of Dutch military IT platform services with the *conceptualized cyberspace* and 'Bowtie' methodology models the risks with cascading effects to each cyber domain layer. Cybersecurity controls (norms) are then proposed to the Dutch military supervisory body within an appropriate risk treatment strategy from a governance perspective.
The remaining design requirements imply high interactions within the governance layer for supervising the management of cyber security risks: (2) cooperation between relevant supervisors, (3) harmonizing their control frameworks, (4) collection of information for supervising compliance monitoring and risk management, and (5) intervention (if needed).

Subsequently, "*the integrated cybersecurity supervision model for the Dutch military*" models an integrated risk-driven approach for supervising the owner (management), operation/support, provider, and SBB layers. The (visualisation of the) cacsading effect using the "Bowtie" for the socio-technical and technical layers is inspired by the master thesis "Can NL trust 5G?" by Farley Wazir. [9] Cooperating supervisors share information (such as applied control frameworks, accepted risk levels, and interventions). The objective is to ensure trust with Dutch military stakeholders by demonstrating end-to-end security for the adjacent cyber subdomains (risks with cascading effects) supporting Dutch military and partner units.

[1] Random security tests: desk research (setup), acceptance tests (existence), or penetration tests (exploitation).



*Dutch military one-tier BOD: composed of senior (non) executive directors

THE PROPOSED INTEGRATED CYBERSECURITY SUPERVISION MODEL FOR THE DUTCH MILITARY DOMAIN

Following the Hevner design science guidelines, the Dutch military cybersecurity supervision model is evaluated based on (interim) approvals for operating fourteen Dutch military-critical IT platform services issued by the BA. [10]

In practice, organization-wide implementation of a compliance and risk management system as part of the owner/management layer (with cybersecurity as one of the aspects) appears insufficient. As a result, implementing the integrated cybersecurity supervision model for the Dutch military domain is not entirely possible. In that case, the focus remains on time-consuming checks of many cybersecurity controls (symptoms treatment) rather than systematic risks.

However, the evaluation also shows that the model can be used to grow into an effective compliance and risk management system (and improve cybersecurity situational awareness and sensemaking). The result will ultimately be a fully integrated cybersecurity supervision model for the Dutch military domain.

Contents

1 Introduction

Innovative civilian technologies entering the military sector [11] are becoming more critical for military (cyber[2]) operations [12] [13] and information sharing within back-office environments. Information Technology (IT[3]) and Operational Technology (OT[4]) services provide value to military operations and their supporting units. The "*consumerization*" [14] of these technology services expect to deliver better performance and productivity gains. [15] [11] However, participating in cyberspace is not without security risks. These cybersecurity risks may backfire and challenge the Dutch military's expected advantage over the enemy. This introduction highlights the cybersecurity governance challenge of the Dutch Military (1.1) due to the *"digital transformation*[5]*."* After the problem definition & research objective (1.2) comes the research methodology & approach (1.3), and thesis structure (1.4). For a better understanding, the introduction offers a compact description of the Dutch military cyber domain and its actors with many new, complex notions and visualizations, which will be further illuminated in the following chapters.

1.1 The Dutch military cyberdomain and security governance challenge

This section briefly describes the Dutch military cyber subdomain with critical assets to be protected and the relevant actor roles. Then, it highlights the cybersecurity governance challenges and the importance of cybersecurity supervision. When sketching the cyber domain, a few models and visualizations pinpoint the relevant actors and their roles in governing cybersecurity. Organizations expect to benefit from the new opportunities that *digital transformation* offers. [6] As an illustration, consider the business opportunities cloud services and big data analytics have provided to Booking.com and Uber, impacting sectors such as the hotel and transportation industries. The provisioning of IT (platform) services can be described and modeled in a *conceptualized cyberspace* [3] see Figure 1.

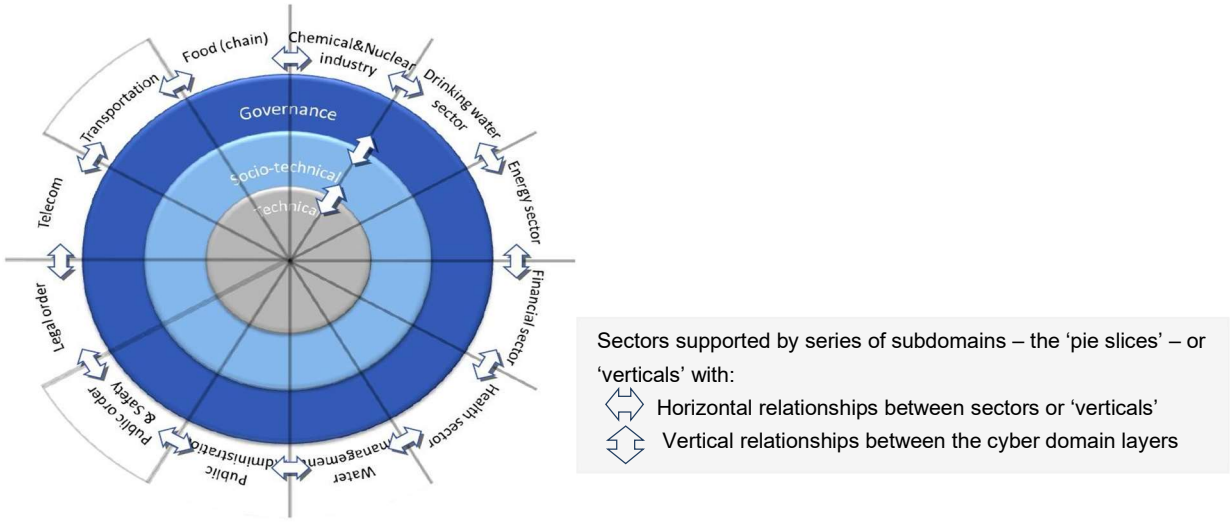


FIGURE 1 CONCEPTUALIZATION OF CYBERSPACE BY VAN DEN BERG ET AL. [3]

Cyberspace matches the structure of a three-layer model, with the middle layer being the socio-technical layer that models *'cyber activities'* (equal to IT-enabled business processes) executed or initiated by users (where certain cyber processes, such as in OT, are fully automated). The technology layer provides the necessary IT infrastructure services to enable cyber activities. Finally, the

[2] MCO: Military Cyber Operations are Intelligence, Defense, and Attack activities in cyberspace (besides *the real world*) to maintain freedom of action and /or create effects to achieve a commander's military goals. [13]
[3] IT: Information Technology.
[4] OT: Operational Technologie systems are, for example, civil Supervisory Control And Data Acquisition (SCADA) systems or Programmable Logic Controllers (PLCs). [100]
[5] Digital transformation: refers to the adoption of digital technology by a company to improve business processes, value for customers, and innovation. [101] [102]

governance layer describes the management of the socio-technical and technical layers and supervises compliance with laws and regulations. See also sections 2.1 and 2.2. Furthermore, this conceptualization divides cyberspace into a series of subdomains - the 'pie slices' - or ('verticals') supporting sectors such as Transport, Telecom, Public Administration, and the (Dutch) Military: see Figure 1. The conceptualization also reveals the horizontal and vertical dependencies between sectors and cyber subdomain layers. [3] Horizontal agreements, for example, between owners of a (series of) subdomain(s) that exchange law-related (e.g., state secret or privacy) information. We now use this cyberspace model to describe, per layer, the Dutch military cyber subdomain, followed by the related cybersecurity governance challenges.

Governance layer (actors and their roles)

The official Dutch military governance directive "Governance of Defence" [16] happens to align precisely with the governance layer of the 3-layer cyberspace conceptualization. [3] The directive explains the governance implementation within the Dutch government's political decision-making context: see also section 2.3. The Dutch military governance directive describes three leading *decision-making roles*:

The Secretary-General (SG) is ultimately responsible for (1) Strategy[6] *& policy, the Chief of Defence (CHoD) is responsible for (2) coordinating its implementation, and the* commanders/*directors (CDT/DIR) are responsible for (3) the implementation by executive units.* [16]

The *"IT platform organization"* concept visualized in Figure 2 is used for pinpointing the (decision-making) actors and their roles in the Dutch military cyber domain. The concept models organizations as an ecosystem with the same basic structure and four actor roles creating value for each other. [17] The concept aligns with the Dutch military strategy in which innovative technology transforms the organization by introducing new business models for creating value. [12] [18] The SG and CHoD are part of the departmental (highest) *governing body* and mandate ownership for business process domains and associated IT platform services at strategic and structure/operations levels, respectively. [16] Figure 3 is based upon "A generic framework for the business-IT relationship" [19] and depicts the IT platform actor roles on the three cyberspace layers introduced. For example, the decision-making owner role is part of the governance layer at the three levels. See for more details subsections 2.2.1 and 2.3.1.

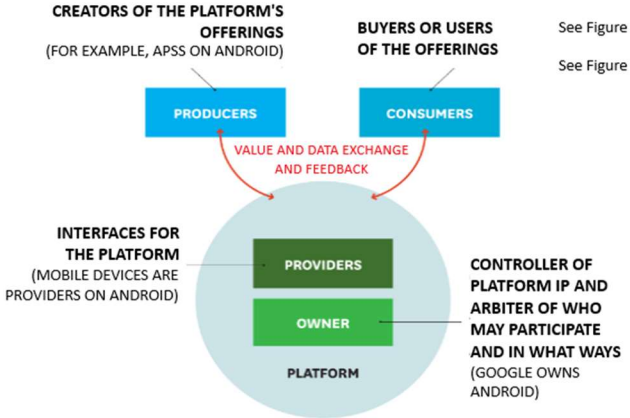


FIGURE 2 IT PLATFORM ORGANIZATION ACTORS

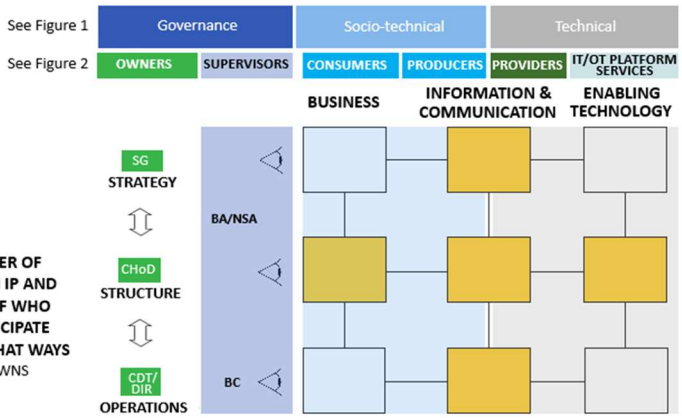


FIGURE 3 INSPIRED BY "A GENERAL FRAMEWORK FOR THE BUSINESS-IT RELATIONSHIP"

[6] Dutch military strategy: the leading objectives align with the mission *"to protect what is valuable to us"* depicted by the Constitution (Article 97) [103] and laid down in the charter for the Kingdom of the Netherlands. [16]

The IT platform service owner manages the 'verticals' of Figure 1, such as the Dutch military cyber subdomain. Governance becomes evident by answering the (a) what/why, (b) how, and (c) result questions: (a) setting up a cyber strategy, regulatory framework & roadmap by the SG, (b) coordinating the implementation by the CHoD, and the (c) CDT/DIR executes the roadmap, monitors results & reports to the *governing body* (via the CHoD). Figure 3 also depicts (in the left column) the mandated Dutch military *supervisor roles*: Departmental Security Authority (BA[7]), Organizational Security Coordinator (BC[8]), and the Dutch Military National Security Authority (NSA[9]). [16] These roles stem (mandated by SG) from the "Decree Security Officer (SO) structure civil service 2021." [20] The supervisor oversees the socio-technical and technical layers from the governance layer perspective. The mandated independent supervisor contributes to the actor/stakeholder's *trust*[10] in the security of cyber activities and (provided) IT platform services, with the mandated business owner responsible.

Socio-technical layer (actors & critical assets)

According to the Dutch military business *value chain*[11]*,* [16] the effective deployment of the Dutch military is only possible through a good combination of three core business processes/activities:

(a) Governance/Command & Control (C&C), (b) Readiness & Deployment, and (c) fulfilling personnel & material needs. [16]

Following the IT platform concept, the users (producers & consumers) of Figure 2 engage in the three core business processes/activities to generate the expected value (benefits) for one another and the platform organization as a whole. [17] We also use the cyberspace three-layer model (Figure 1) to map the Dutch military value chain on the socio-technical layer. The description of the socio-technical layer then follows from the three core business processes/activities (value chain) enabled by the provided IT platform services. Thus, the cyberspace conceptualization (only) describes the Dutch military's IT platform service-enabled core business processes/activities. Many of these core processes/activities are suitable for adding value to the Dutch military through innovative IT platform services. Actually, cyber activities are considered *critical assets* of the socio-technical layer for adding value to the Dutch military. For example, innovative civilian IT is expected to improve governance activities based on information-driven decision-making by using critical aggregated business management data.
The use case also takes off when these *(a) governance* activities merge into *C&C* information-driven activities coordinated by the ChoD during military missions or exercises.
Next, *(b) Readiness & deployment* activities executed on behalf of the CDT/DIR jointly shape the military *operational processes.* The combination of personnel & material readiness and exercise activities leads to operational-ready units that determine the deployability of the Dutch organization as a whole. These military *operational processes* are suitable for adding value through innovative IT platform services. For example, cyber activities support information-driven tactical decision-making (C&C) for units on a mission, such as border patrol units at Schiphol Airport or deployed Air Force units. [13] [21] Other examples are military *operational processes* enabled by military cyber-attack operations performed by the Defence Cyber Command (DCC) subunit [13] or INTEL cyber operations performed by the Military Intelligence & Security Service (MIVD).

[7] BA: Beveiligings Autoriteit.
[8] BC: Beveiligings Coordinator.
[9] NSA (National Security Authority): responsible for the security of NATO and EU classified information from other international partnerships & treaties and to conducts periodic inspections. [16]
[10] Trust: is defined as a necessary condition for realizing the expected benefits. [1]
[11] Value chain: a collection of activities that are performed by a company to create value for its customers. As a result, the added value leads to competitive advantage *(*Porter et al.). [104] [105]

Finally, the *(c) fulfillment of personnel & material needs* activities executed by the supporting units (on behalf of the CDT/DIR) are also known as the *supportive (business) processes* and conditional for the *operational processes.* Consequently, cyber activities executed by these supporting units are equivalent to the *supporting processes* and thus form a dependent sub-layer for the fundamental military *operational processes* (composed of *Readiness & Deployment* activities).

Technical layer (actors & critical assets)

The IT platform actor shown in Figure 2 is the IT service provider acting as the interface between the provided innovative IT Platform services and its users. More specifically, the provided IT platform services enrich information to add the expected user value, such as enriched NATO secret or national state secret information. In other words, the IT services give more meaning to the national or NATO information to enable the Dutch military *operational & supporting* processes. As a result, in addition to the critical cyber-activity assets, information processed by IT services at the technical layer is also regarded as a critical asset for adding value. For this reason, cyber activities and information processing cannot be viewed in isolation in adding value to an organization from the governance layer perspective. Therefore, the IT service provider enters into vertical agreements with IT platform owners depicted in Figure 1. A Service Level Agreement (SLA) on the quality/reliability of the IT platform services and their supervision ensures the stakeholder's critical trust in enabled *operational and support* activities (processes) to add value to the Dutch military. The SLA addresses the vertical relationship between the IT platform owner (governance layer) and the operational & supporting cyber activities (socio-technical layer) dependence on the IT platform supplier (technical layer). Figure 4 provides an impression of the Dutch military sub-domain technical layer, along with some examples of IT platform services, such as C&C information-driven or INTEL IT platform services, allowing previously stated operational use cases. [22]

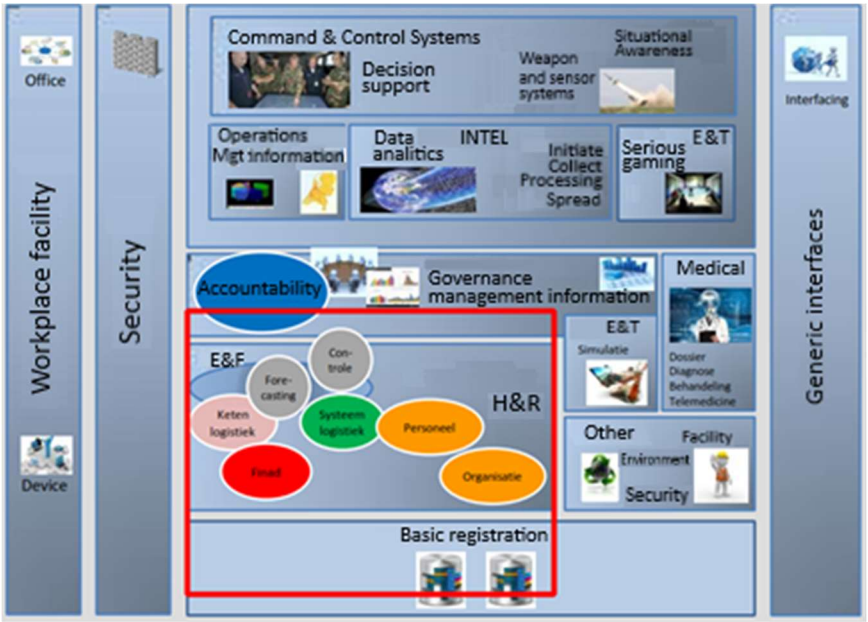


FIGURE 4 IMPRESSION OF THE LANDSCAPE OF EXISTING IT SERVICES [22] ALIGNED WITH EAR[12] AND NISP[13] STANDARDS

Business management information and Education & Training (E&T) IT services allow supporting use cases. As shown in the red box of Figure 4, other examples are enterprise-wide IT platform services adding expected value for generic E&F/HR&O[14] use cases. For example, these IT services comprise

[12] EAR: Enterprise Architecture Civil service provides a coherent description of the organization and design of the information services and facilities of the Central Government. [55]
[13] NISP: NATO Interoperability Standards and Profiles. [106]
[14] E&F/HR&O: Equipment Logistics & Finance / Human Resource & Organization.

civil commodity software and hardware components from vendors such as SAP and Peoplesoft using linked enterprise-wide basic registration services. Furthermore, Figure 4 presents security and workplace IT platform services such as Identity & Access Management (IAM), commodity (Microsoft) office software/cloud platform services, and mobile phones or tablets supplied by telecom providers. Finally, on the right, the figure shows interfacing network services to exchange critical information to add the expected value to its users and the Dutch military.

The cybersecurity governance challenges

After sketching the cybersecurity domain and its actors, this section briefly lists the cybersecurity governance challenges due to participation in cyberspace and resulting security risks, further elaborated and illuminated in the following chapters.

First, adding value for IT platform users (socio-technical layer) is hampered due to a lack of standardization of the growing number of interfaces between the (initially) isolated networks (technical layer). Deloitte research states that step-by-step innovation programs for *digital transformation* to an integrated Service Oriented Architecture (SOA) will take years. [23] [24]

Secondly, the extensive landscape of adjacent cyber subdomains aimed at adding value creates a large and growing attack surface. State actors deploy cyber attacks that might exploit vulnerabilities to breach the security of critical (but initially isolated) cyber subdomains to achieve their geopolitical goals. According to the '*Cyber Security Assessment Netherlands 2023,'* [25] the threat to the Netherlands remains unabatedly high and dynamic and may backfire on the expected advantage over the enemy. Due to the rapid digitization, keeping users up-to-date and getting users to adopt a permanent cyber security attitude in their work is a challenge. Ideally, users are unknowingly cybersecurity-skilled. Governance challenges arise in creating a corporate cybersecurity culture in the military domain around the users (as part of the socio-technical layer) of IT platform services.

Thirdly, the *trade-off* by mandated owners (governance layer) between threats and value creation (such as combat power) determines the required reliability for IT platform services and prevention and correction controls. Subsequently, the required controls following the *trade-off* must comply with regulations and, therefore, also determine whether a use case takes off at all. [22]

Finally, in the past, when isolated networks and applications of the technical layer were managed locally, user trust in security was implicit and relatively simple. On the other hand, due to the growing number of interfaced IT services, evolving threats, stakeholders, and managers (decision-makers) for risk handling, collecting information for supervising compliance becomes challenging. However, independent *cybersecurity supervision* is essential to the trust in IT platform services by its users, partners, and society. Trust in the layered infrastructures is a necessary condition for realizing the expected benefits. [1] Given the various developments mentioned, supervising risk handling and compliance with regulations to maintain the trust of Dutch military units, partners, and society in end-to-end cybersecurity is not as straightforward from a governance perspective as it used to be.

1.2 Research Goal

As explained above, the 3-layer cyberspace conceptualization [3] makes the following sharp distinction: *cybersecurity* concerns the security (securing) of the cyber activities or cyber processes (i.e., the security of the socio-technical layer), and *information security* is the security of the technical layer (in terms of CIA[15]). [3] The focus is on the integral[16] cyber security supervision viewed from the governance layer perspective. This thesis examines governance and, more specifically, cybersecurity supervision challenges within the Dutch military domain's rapidly changing digital environments. Within this view, managing existing and newly upcoming cybersecurity risks by operational and supporting units also requires an integral supervision approach. The overall objective is to design an

[15] CIA: the reliability aspects for Confidentiality, Integrity and Availability.

[16] Integral cybersecurity supervision: cooparating supervisory bodies at the state, sectorial and organizational levels aimed at (trust in the) end-to-end security of IT platfom services.

integrated approach for supervisors to ensure stakeholder trust[17] (Figure 1).
Based on these observations, the main research objective is:

"to design an integrated cybersecurity supervision model for the Dutch military subdomain."

The innovative civilian technologies entering the military sector, together with the related increasing number of cybersecurity threats, are the starting point for the scope of the thesis.

1.3 Research methodology and approach

The Hevner et al. design science methodology [8] will be used to design the integrated cybersecurity supervision model (as a viable artifact). The methodology enables systematic exploration of the *problem domain* and evaluation of the model (artifact). Figure 5 shows a refinement of the Hevner methodology by viewing design science as a *mutual nesting* problem-solving approach [26] (trial and error). The approach searches for a *possible solution* by integrating the three boxes in Figure 5: *Environment, Information System (IS) design science*, and *Knowledge base*.

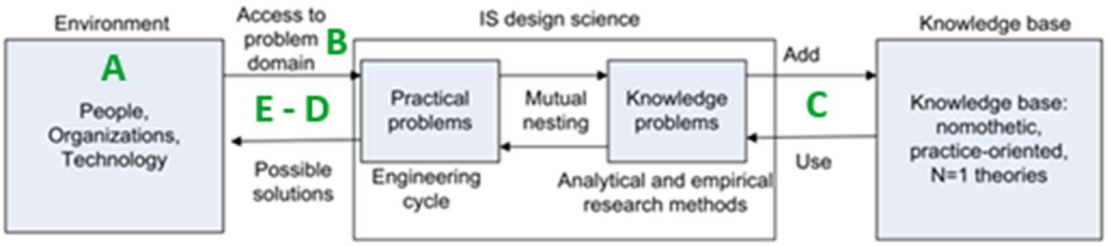


FIGURE 5 DESIGN SCIENCE AS NESTED PROBLEM SOLVING: REFINEMENT OF THE HEVNER FRAMEWORK [26]

We now use the refined Hevner methodology, as visualized in Figure 5, to sketch the way our research has been organized.
The *digital transformation* of the (A) Dutch military environment and resulting cybersecurity (B1) governance & (B2) supervision praktical problems (challenges) result in (C1) knowledge problems. By applying research methods to tackle these knowledge problems, the execution of the engineering cycle results in identified (C2) design requirements. After that, these requirements are input for (D) building the integrated cybersecurity supervision model (potential solution). The next step (E1) verifies the model (artifact) based on a design evaluation, followed by the final (E2) conclusions, reflections & recommendations.
APPENDIX A delves deeper into the design science steps in Table 1 following the Hevner guidelines.

(A)	Dutch military environment;
(B1)	Cybersecurity governance challenges for the Dutch military cyber domain;
(B2-C)	Cybersecurity supervision challenges and model requirements (governance perspective);
(D-E1)	Building the cybersecurity supervision model and evaluation;
(E2)	Conclusions, reflections, and recommendations.

TABLE 1 STRUCTURE OF THE THESIS BASED ON THE REFINED HEVNER FRAMEWORK (PRESENTED IN FIGURE 5)

1.4 Structure of the thesis

This thesis is structured around the design objective and the related design science steps (A-E) presented in Figure 5: each design science step is covered by a chapter. The last chapter covers this thesis conclusions and recommendations.

[17] Stakeholders: groups and individuals who, directly or indirectly, influence – or may be influenced by – the attainment of the company's objectives: employees, shareholders, other lenders, suppliers, customers, and other stakeholders. [2]

The thesis chapters are:

Chapter 1: Dutch military environment & thesis problem definition (A);
Chapter 2: Governance challenges for securing the Dutch military cyber domain (B1);
Chapter 3: Supervision challenges for securing the cyber domain (governance view) (B2-C);
Chapter 4: Cybersecurity supervision model (D) and validation (E1);
Chapter 5: Reflections, conclusions, and recommendations (E2).

The basic structure of the thesis is presented in Figure 6.

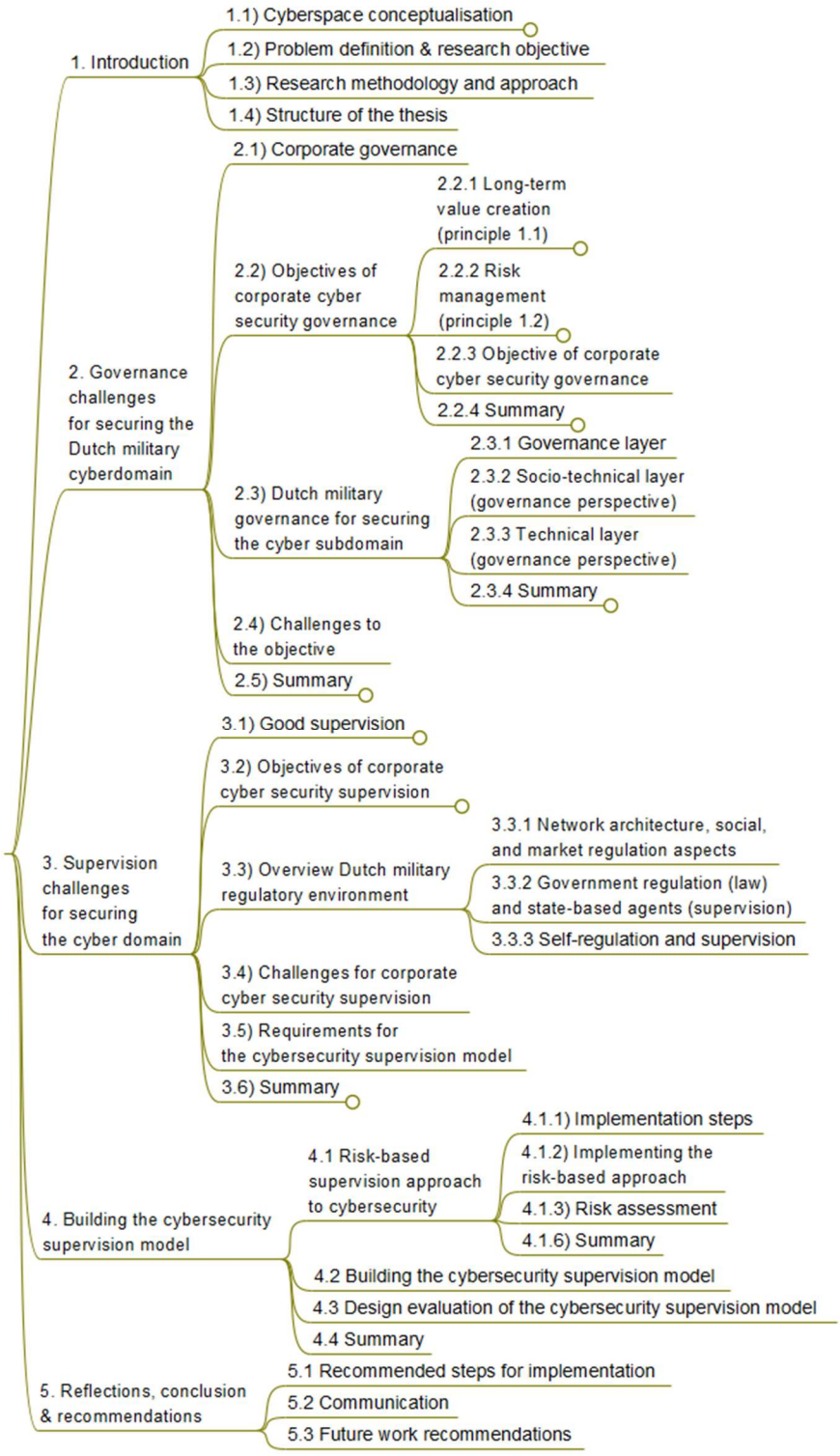


FIGURE 6 STRUCTURE OF THE THESIS

2. Governance challenges for securing the Dutch Military cyber subdomain

This chapter examines, in more detail, the challenges for securing the cyber subdomain from the governance perspective of the (large) IT platform organizations hereof the Dutch military subdomain. First, section 2.1 defines corporate governance. Section 2.2 then identifies general corporate governance objectives (principles) relevant to handling cybersecurity, followed by section 2.3 describing the Dutch military "problem domain" for governing cybersecurity. Subsequently, section 2.4 analyzes the "problem domain" and identifies the challenges in managing existing and newly upcoming risks (due to value creation).

2.1 Corporate cyber security governance

The Dutch Monitoring Committee drew up the "Dutch Corporate Governance Code" (December 2022) [2] and defined corporate governance as:

" Management & control, about responsibility and influence, and about supervision and accountability." [2]

Corporate governance involves establishing policies and continuous monitoring of their proper implementation by the members of the *governing body*. A one-tier[18] (besides two-tier[19]) *governing body* composed of executive and non-executive directors is named a Board Of Directors (BOD) and serves to "*direct and control"* an organization[20]. The composition and operation of the BOD must be such that supervision by non-executive directors is exercised appropriately and independent supervision is guaranteed.
The executive directors typically oversee day-to-day operations, and the non-executive directors represent, among others, the interests of employees, producers, consumers, shareholders, and society as a whole. The Code is a form of self-regulation for private sector organizations and supplements government regulation, further elaborated in section 3.1.
The so-called regulatees[21] develop self-regulatory procedures and policies based on the Code principles. The regulatees adhere to the Code principles in the light of more general public policy objectives following the multi-stakeholder model. [7] [2]
The BOD members of the regulated organization account for compliance with the Code in the general meeting. For this, the members provide a substantive and transparent explanation to their shareholders for any departures from the Code principles and best practices.
The explanation to the shareholders follows the "comply or explain" principle and is essential for the relationship to cybersecurity. Based on this, BOD members must understand cyber threats for their organization and whether they are making sufficient adjustments to achieve their strategic objectives. The IT platform concept models organizations as an "*ecosystem*" where cooperating actors follow a strategy for value creation.[17] To keep this collective strategic goal of value creation achievable, the BOD members of the IT platform organization must manage the risks resulting from the larger attack surface. The extent to which adjustments are sufficient for the long and short term depends on the *trade-off* between the expected added value (such as combat power) and the associated increased cybersecurity risks (1.1). [27] For a transparent trade-off, representation of all relevant stakeholders and independent supervision is crucial for gaining mutual trust.
Therefore, the "Long-term value creation," "Risk management," and "Role of the supervisor" code principles are relevant for corporate cybersecurity governance.

[18] Board of Directors (BOD): one-tier *governing body* consisting of executive and non-executive directors. [2]
[19] Supervisory & Management Boards (SB/MB): two-tier *governing body* comprising a Management Board with executive directors and a Supervisory Board with non-executive directors. [2]
[20] Organization: the terms 'organization' and 'corporation' are identical in this thesis and used interchangeably.
[21] Regulatees: regulated parties such as addressed by the Dutch Corporate Governance Code. [2]

2.2 Objectives of corporate cyber security governance

This section further explains the objectives for securing the cyber domain based on the Code's principles of “Long-term value creation” (2.2.1)and “Risk management” (2.2.2). (Chapter three further elaborates on the “role of the supervisor” principle). An overview of the objectives (2.2.3) and summary (2.2.4) finalizes this section.

2.2.1 Long-term value creation

Principle 1.1: the BOD executive directors are responsible for the organization's continuity and sustainable long-term value creation, take into account the impact of its actions on people and the environment, and, to that end, weigh the relevant stakeholder interests in this context. [2]
The BOD *e*xecutive directors set the *strategy* for “long-term value-creation,” a feasible roadmap about “what” needs to be done with “*boundary conditions*[22]*”* for its implementation, organizational structure, and a regulatory policy framework. Compliance with the regulations within the established *boundary conditions* requires continuous monitoring and performance reporting at the operational and tactical levels. Non-compliance impacting "*long-term value creation*" may require strategy adjustment and justification by BOD members to its shareholders at the general meeting.

Business-IT platform services alignment and governance

As IT platform services become increasingly intertwined with business activities aimed at *long-term value creation*, cybersecurity governance is essential for connecting business activities and cybersecurity objectives. The IT platform *strategy* (and roadmap) aims to create more value for IT platform service providers and users (producers and consumers) through data exchange, as shown in Figure 2. [17] For this, Partner organizations in the Public (such as the Dutch military) and Private sectors (PPP[23]) increasingly cooperate towards agreed objectives (“strategy”) for creating value for each other. [28] The *boundary conditions* are the starting point for the “*mandated business owners*[24]*”* at the tactical (“how”) and operational (“result”) levels responsible for coordinating the execution of the roadmap. The existing field of business & IT alignment (see APPENDIX B) is in line with the layers often defined within the Enterprise Resource Planning (ERP[25]) framework: the business layer (business processes), the application layer (IT services), and the technology layer (of enabling technologies). [3] Figure 3 maps the decision-making business owner role to the three governance levels.

Governance Direct Control cycle for managing compliance with regulations

Before the explosion of the number of end-users, the focus of (mainly) technical managers was on correctly implementing the IT (platform) services preventive & repressive controls part of the technical layer and measuring the effectiveness through continuous monitoring. Information Security (IS) Governance involves the strategic, tactical, and operational levels based on regulations[26]. Across these three levels, the organization directs, executes, and controls actions. [27] To get the desired result, the *executive directors* may adjust their strategy based on feedback from the (mainly) technical managers at the tactical and operational levels (see Figure 3 and APPENDIX B. For this,

---

[22] Boundary conditions: determined by conditions such as the (security) regulation framework, available financial, human, social, and technological resources, and implementation timeframe.
[23] Public Private Partnership (PPP): involves cooperation between one or more organizations from Public administration and the Private business community, working together towards agreed objectives. [107]
[24] Mandated business owners: mandated by BOD executive directors.
[25] ERP: Enterprise Resource Planning is the integrated management of main business processes, often in real-time and mediated by software and technology. [108]
[26] Governance (IS) regulations: directives (strategy level), policies & company standards (tactical level), and procedures & guidelines (operational level). [29]

operational units report *operational data*[27] to the tactical manager to check for adequate procedures. Next, the tactical manager reports *Infosec Process data*[28] to the strategic level. Governance staff at the strategic level analyze the *Infosec Process* data and report relevant *Performance info*[29] to the *governance board executive directors* to evaluate the progress for possible adjustments. [29] In other words, evaluating the progress of implementing Information Security (IS) controls through a compliance management system (BOD executive director perspective). Figure 7 visualizes the "Von Solms and Von Solms IS Governance[30] Direct Control cycle[31]." [27]

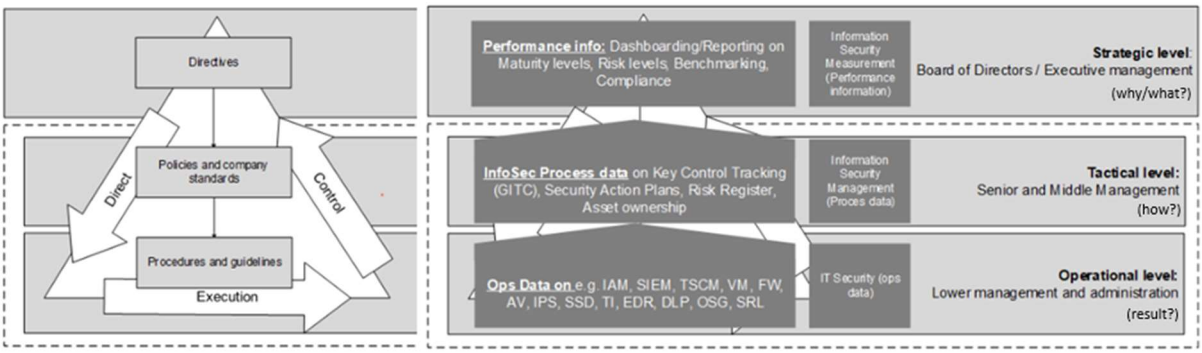


FIGURE 7 INSPIRED BY IS GOVERNANCE DIRECT CONTROL CYCLE - VON SOLMS AND VON SOLMS (2006) [29]

2.2.2 Risk management

Principle 1.2: The organization should have internal risk management and control systems with the executive directors responsible for identifying and managing the risks associated with its strategy. [2] Until many years ago, organizations mainly focused on securing the technical layer of their cyberspace environment. However, innovative civilian technologies entered the military sector, networks became increasingly interconnected, and applications became more and more user-friendly and intertwined with the socio-technical layer of cyber activities and business operations. Subsequently, the number of users & assets[32] accessible through cyberspace exploded. [3] Therefore, cybersecurity also includes securing assets reachable through cyberspace and securing activities initiated by people and processes as part of the socio-technical layer. Von Solms and Von Solms state that:

"The security of cyberspace is not only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace." [30]

The statement is consistent with the sharp distinction made by Van den Berg et al. between Information Security and Cyber Security when taking into account that the cyberspace definition by Von Solms is more limited than the more holistic cyberspace definition by Van den Berg et al. See section 1.2. [3] Accordingly, following the holistic view on cyberspace by Van den Berg et al., the cybersecurity of IT platform services is broader than just about the security of IT, but about the cybersecurity of people, processes, and technology, with security governance (based on corporate strategy and design) as the overarching layer. [31] [32] [33] Hence, users (producers & consumers) in the socio-technical layer with knowledge about the enabled cyber activities are responsible for

[27] Operational data: collected from for example Security Information and Event Management (SIEM) or Identity access management (IAM) security (sub) systems. [29]
[28] Infosec Process data: General IT Controls (GITC), Security Action Plans, Risk Register or Asset Ownership. [29]
[29] Performance info: Dasboarding/reporting on e.g., Maturity & risk levels, Benchmarking or compliance. [29]
[30] IT/IS governance: APPENDIX C presents examples inspired by the IS governance *Direct Control* cycle. [93] [94]
[31] *Direct Control* PDCA *cycle*: Direct (PLAN), Execution" (DO/ACT") & Control (CHECK). [36] See APPENDIX D.
[32] Assets: Information & Operational Technologie (IT & OT) or cloud-based assets. [100]

thinking about the security of their actions. [3] Consequently, standardization bodies[33] added cyber risk management security controls to their Communication and Information Security (CIS) standards. ISO defines Risk Management as:

"Coordinated activities to direct and control an organization with regard to risk." [34]
In other words, risks that could prevent (IT platform) organizations from executing their strategy for long-term value-creation (principle 1.1) also require Cyber Risk Management (Principle 1.2).
Based on the IS governance Direct Control cycle, BOD executive directors are ultimately responsible for designing and implementing adequate IT (platform) service controls in the technical layer. However, given the rise of cyberspace with its explosion of users & assets accessible through cyberspace, what is the impact if prevention & repression controls in the technical layer fail? Van den Berg et al. state:

"Information Security breaches occur in the technical layer, while the true impacts (risks) of these breaches work out into the socio-technical layer of cyber activities." [3]

Thus, the impact (risks) of IT platform service security breaches works out into the business operations part of the socio-technical layer of cyber activities.

The "Bowtie"

The Cyber Risk Management Cycle entails (a) identifying the *critical assets*[34], (b) identifying & assessing their risks for the organization, (c) defining acceptable risk levels (low-hanging fruit first), (d) deciding ways (accepting, avoiding, mitigate, transfer) of dealing with risks, and (e) designing & implementing risk measures in all cyberspace layers. Moreover, the Cyber Risk Management Cycle also entails (f) monitoring the effectiveness of implemented controls (using cyber situational awareness and sensemaking). [34] In Figure 8, the model visually represents the relationship between threats, prevention controls, (inter)dependent incidents, repression controls, and impact (risks).

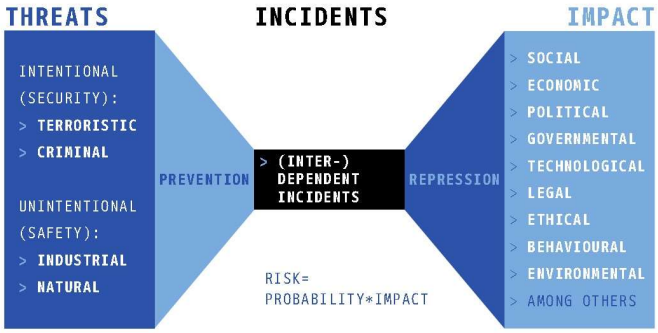


FIGURE 8 CYBER RISK MANAGEMENT USING THE 'BOWTIE' [3] [35]

The implemented controls are expected to mitigate risks to acceptable levels for the IT platform organization, with risks defined as the product of *probability* and impact. The risks are unacceptable for *executive directors* (and *mandated business owners)* when the (*probable*) impact hinders the strategy for long-term value creation. The Bowtie model visualizes *probable* scenarios around (inter) dependent incidents caused by unintentional (safety) and intentional (security) threats.

[33] Standardization bodies: such as the International Standardization Organization (ISO), NIST, and NATO Security Committee (see also section 4.2). [33] [79]
[34] Critical assets: critical cyber activities enabled by IT platform services processing critical information.

Risk management and control systems (considering cascading effects)

Failed controls may lead to security breaches and (inter)dependent incidents, triggering *systemic risks*[35] with cascading effects into adjacent subdomains supporting the Dutch military and partner units. A security breach in an infrastructure cloud service provider can be considered as a threat to the security of an application service provider in the technical layer. Next, a breach in the security of the application service provider is also a threat, with the actual impact (risk) of the breach working out into the socio-technical layer of cyber activities. Subsequently, mandated IT platform service business owners (Figure 3) may be unaware of the criticality of their service to service owners in adjacent subdomain layers (or vice versa). The lack of risk awareness requires risk management that takes the cascading effects of adjacent subdomains into account.
In addition, risk management is an ongoing process. Therefore, identified changes in any facet will necessitate updating and re-evaluating the acceptable risk levels (and adequate security controls) by the various IT platform service owners involved. Subsequently, BOD executive directors are ultimately responsible for designing, implementing, and maintaining an organization-wide (cyber) risk management and control system (principle 2.2.2), with the control system inspired by the IS governance *Direct Control* cycle shown in Figure 7. [36]

Situational Awareness & Sensemaking

Situational Awareness (SA[36]) & Sensemaking[37] can support effective risk management for complex environments with adjacent cyber subdomains. For robust decision-making (long-term) regarding value creation, the BOD executive directors focus on understanding (looking back) and adjusting strategy when risks are too high based on Sensemaking. In contrast, SA supports agile decision-making (short-term). [37] [38]

2.2.3 Objective of corporate cyber security governance

Aligning the (a) principles of the Dutch Corporate Governance Code (long-term value creation, risk management, and role of the Supervisor) with the (b) cyberspace conceptualization by van den Berg et al. (three-layer model), the (c) actors of the IT platform services (owners, consumers, producers, and providers), the (d) generic framework for the business-IT relationship (actors at strategy, structure/tactical, and operations levels), (e) the governance direct control cycle (compliance management), (f) the "Bowtie" methodology (cyber risk management), and (g) Endsley (SA & sensemaking) the conclusion is that objectives for securing the cyber domain can be recapitulated as follows:

(1-a/b/c/d) Long-term value creation versus cyber security trade-off, (2- e) managing compliance of cybersecurity controls based on the governance direct control cycle, (3-a/f) managing systemic (cascading) cyber risks, and (4-g) adjusting to stay in control in the event of non-compliance.

2.3 Dutch military governance for securing the cyber subdomain

In this section, a tight overview of the Dutch military cyberspace layers using the governance perspective is provided.

[35] Systemic risks (with cascading effects): the possibility that a single event or development (caused by the system, organizational design, or culture) might trigger widespread failures and negative effects spanning multiple organizations, sectors, or nations. [31] [109] [110]
[36] Situational Awareness (SA): Endsley points out that SA typically looks ahead and projects what is likely to happen to inform effective short-term decision-making processes. [37] [38]
[37] Sensemaking process: is backward-focused, forming reasons and understanding for past events. [37] [38]

2.3.1 Governance layer

The Dutch military mission is "*to protect what is valuable to us"* in a rapidly changing world. Therefore, a resilient Dutch military organization is required to face threats and seize opportunities, as outlined in the "Defence Vision 2035", [39] "Defence Directive 2018", [12] & "Defence IT Strategy 2019 – 2024." [18] The Dutch military established regulations supporting the mission, strategy, and decision-making through the "Governance at Defense Directive" [16], a form of self-regulation. The directive principles align with the Dutch Corporate Governance Code principles for private sector partners, [2] reflecting widely held general views on good corporate governance. The focus is on "*governance structures*[38]*"* and *"principles & tasks*[39]*."* The directive follows the international development of the governance doctrine (such as [40] [41] [42] [43]). [16] Supreme authority over the Dutch military is exercised by the government and controlled by parliament, based on the constitution. The Ministry of Defense is headed by the Minister of Defense (MOD), part of the government. The Secretary-General (SG) is, with due observance of the instructions of the MOD, charged with the administrative management of the ministry. The Chief of Defence (CHoD) is the highest-ranking military officer who advises the minister. The highest *governing body* is the BOD ("Bestuursraad"), composed of the SG (chairman), pSG (deputy SG), Directorate-General Policy (DGB), Chief of Defense (ChoD), Directorate Finance (HDFC), and the Chief Information Officer (CIO) regarding IT-related subjects. The CDT/DIR presented in Figure 3 heads executive organizational units. The CDT/DIR must comply with defense policy, laws, and regulations. For this, the units should have a compliance management system, one of the Integrated Risk Management (IRM) components. With transparent and up-to-date management information, the executive units provide insight into the realization of the implementation. The insight may include reporting to one of the BOD members (SG or CHoD) on any decision points outside the scope of the engagements or where non-compliance impacts long-term value creation.

The three governance levels shown in Figure 3 correspond with the strategic (why/what?), structure/tactical (how?), and operational (result?) levels. In governing the Dutch military, realizing its policy, results, and effects are central. The realization is achieved by aligning the three governance levels. Control over the functioning of process domains or escalation of bottlenecks in the implementation occurs via the ChoD and process management. Possible escalation may occur to the highest decision-making *governing body,* the BOD.

The Dutch military BOD executive directors mandate ownership of their core business process domains at the strategic level. Next, IT platform services ownership (aligned with the process domain ownership) is mandated at the tactical (structure) and operational levels for roadmap implementation (change) and maintenance (run), respectively.

APPENDIX G visualizes the complex tuning approach using "*integrated control cycles*[40]*"* per governance level. Regardless of the organizational suspension, the Dutch military supervisors have an independent position and direct access to the SG (BOD). See Figure 26. [16] APPENDIX visualizes the important horizontal adjustments between the various process domains & the vertical coherence within the process domains, including escalation steps to the BOD. See Table 11 & Figure 28. [16]

2.3.2 Socio-technical layer (governance perspective)

The effective deployment of the Dutch military is only possible through a good combination of the three core processes/activities represented by (the vertically coherent) process domains[41]. Figure 9 shows the three core businesses in the Dutch military value chain's orange, blue, and green areas, placed within its (inter)national environment, including the Dutch military partners (PPPs) & threats.

[38] Governance structures: see APPENDIX E. [16]

[39] Principles & tasks: see APPENDIX F. [16]

[40] Integrated control cycles: integrally coordinated & executable governcance levels (APPENDIX G).

[41] Process domains: represents the Dutch military three core busines processes/activities with policy, design and implementation roles responsible (mandated by SG, CHoD & CMDs/DIRs), see Table 11 in APPENDIX . [16]

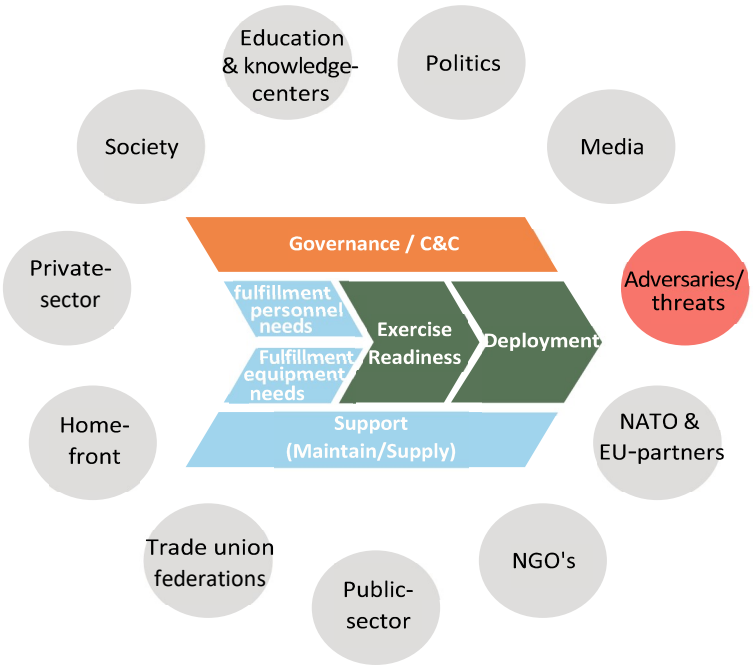


FIGURE 9 DUTCH MILITARY OPERATIONS/SUPPORT VALUE CHAIN, PLACED WITHIN ITS (INTER)NATIONAL ENVIRONMENT

Innovative technologies transform the organization by introducing new business models for creating value, such as information-driven action. The Dutch military IT platform users (producers & consumers) of Figure 2 engage in the three core business processes/activities (value chain) to generate the expected value for the Dutch military. Let us map the value chain on the socio-technical layer of cyber activities (Figure 1). The description of the socio-technical layer then follows from the three core business processes/activities (value chain) enabled by the provided IT platform services. Figure 10 shows a typical information exchange during military missions by deploying a Battlefield Management System (BMS) composed of command posts, vehicles, and weapon systems.

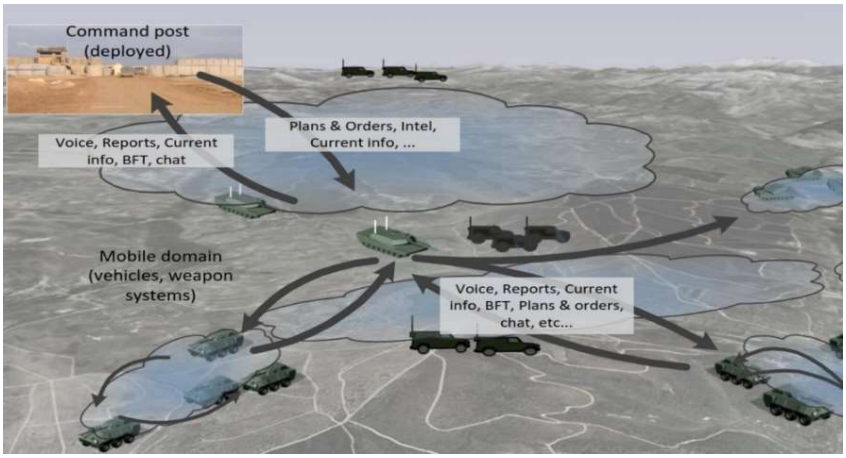


FIGURE 10 TYPICAL BATTLEFIELD INFORMATION EXCHANGE ENABLED BY IT/OT (PLATFORM) SERVICES [44]

The military staff (users) aims to collect information about, for example, friendly and enemy forces from reporting soldiers and sensors. The objective is to create better situational awareness and timely, reliable strategic and tactical decision-making supporting the C&C core deployment process. The BMS equipment fits into different vehicles at each echelon, such as tanks and armored personnel for mobile and on-foot user conditions. [44] [45]
Innovative civilian technologies are expected to allow new stakeholders to exploit many more opportunities for the Dutch military. As a result, the Dutch military BOD members are confronted

with more business proposals from new and traditional stakeholders, which will transform the IT platform organization's value chain.

2.3.3 Technical layer (governance perspective)

This section briefly describes the technical layer composed of IT platform services[42]. The Command, Control, Communication & Computers, Intelligence, Surveillance & Reconnaissance (C4ISR) IT system is a (future) example of innovative IT platform services used by back-office & deployed NATO operations. [46] The C4ISR is the "nervous system" of the military composed of IT platform services defined by cloud and asset-based networks and user devices. The C4ISR example concept shown in Figure 11 is the future BMS through new technologies, such as the hybrid cloud[43] and the combat cloud[44]. [47]

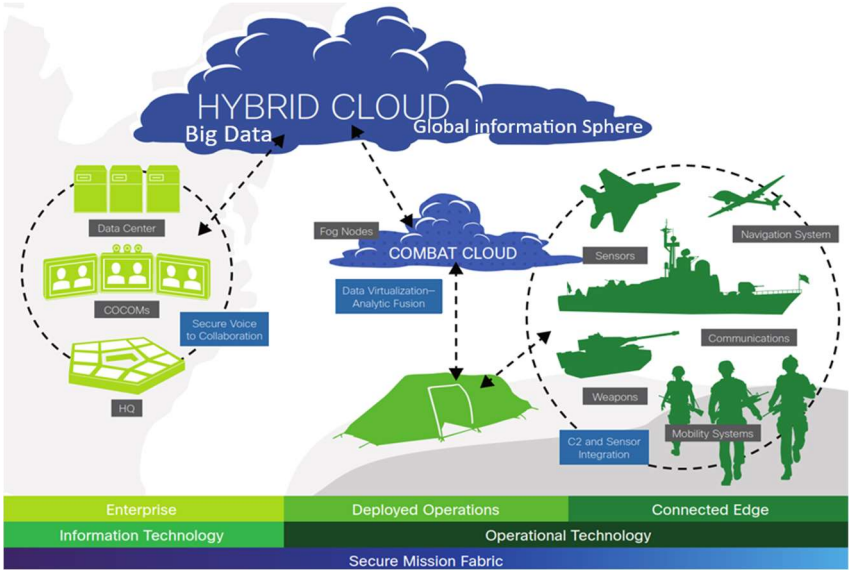


FIGURE 11 THE CONNECTED BATTLEFIELD IN ACTION [47]

C4ISR is the collection of subsystems used to maximize SA and ultimately (sensemaking) plays a crucial role in military strategy & operations. [48] The enterprise back-office IT platform is shown on the left. The center and right parts show the Deployed Operations and the Connected Edge powered by Operational Technology (OT). The deployed operations are, for example, NATO missions deploying joint international naval, army, and air force operations. Cloud computing delivers on-demand network access and demands the availability of high-capacity global interoperable networks. For example, the Service Oriented Architecture (SOA) integrates with the NATO-controlled Federated Mission Networking (FMN) architecture through cloud computing. SOA-based cloud and virtualization solutions decouple network functions from the underlying hardware devices using Network Functions Virtualization (NFV[45]) technology in combination with Software Defined Networking (SDN[46]) technology. [49] With the virtualization of network functions and the decoupling of control and service layers, the focus is now on serving so-called verticals (Figure 1) with custom IT

[42] IT platform services: an IT system (such as C4ISR) composed of cloud & asset-based network & user devices.
[43] Hybrid cloud: is a composition of a public cloud & a private environment, such as a private cloud or on-premises resources, that remain distinct entities but are bound together, offering the benefits of multiple deployment models. [111]
[44] Combat cloud: model for enabling ubiquitous, convenient, on-demand network access to a shared pool of sensors, navigation systems, weapon platforms & C2 functions (aim: force multiplier for shrinking forces). [47]
[45] NFV (Network Functions Virtualization): specific network functions are implemented in software running on generic hardware without the need for certain machines, enabling the sharing and reuse of functionality. [49]
[46] SDN (Software Defined Networking): allows third parties to control network resources and their performance (Complementary to NFV). [49]

services and service levels (reliability), providing greater flexibility and reduced management effort. These technologies ensure the flexible delivery of network services based on an optimally shared physical infrastructure, enabling more economically flexible service additions and network upgrades. It addresses the problem of operational costs for managing and controlling the current "closed and proprietary" appliances by leveraging low-cost commodity servers. [18] [19] Essential components of the cloud model are the three service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). [50] Figure 12 arranges the three cloud computing service models as layers in a stack to visualize vertical interoperability[47] following the NATO Interoperability Standards & Profiles (NISP). [51] From a governance perspective, Figure **13** visualizes horizontal and vertical layered cloud interoperability between NATO and other participating organizations.

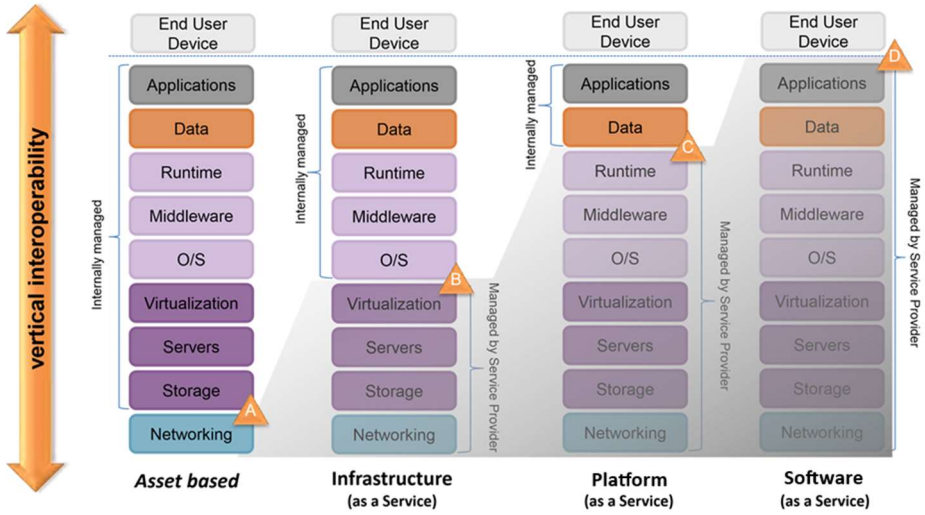


FIGURE 12 INTRA-CLOUD VERTICAL INTEROPERABILITY (FMN VISION) [47]

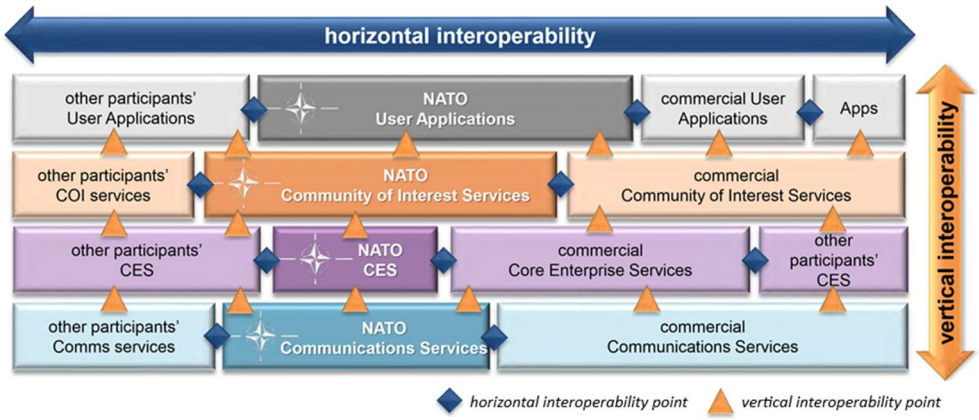


FIGURE 13 - GOVERNANCE PERSPECTIVE: INTRA-CLOUD HORIZONTAL INTEROPERABILITY (FMN VISION) [24] [47]

The orange triangles A, B, C, and D (Figure 12 and Figure **13**) represent the asset-based IaaS, PaaS, and Saas services. The *on-premise*[48] or *off-premise*[49] *managed services*[50] are composed of specific

[47] Interoperability: from the perspective of the intra-cloud, the ability of two systems or clouds to exchange and use information, to use each other's computing resources, to use each other software services, securely and seamlessly, while ensuring security and privacy. [112]
[48] On-premise: services internally managed. [50]
[49] Off-premise: services managed by an external IT service provider such as KPN, NATO, or public sector. [50]
[50] Managed services: user equipment & back-end capabilities (NATO NISP standard), see APPENDIX J)

capabilities. For example, end-user devices & applications (user-facing) or middleware & networking (back-end) capabilities specified by the NATO NISP standard. [51]
The horizontal interoperability (Figure **13**) for the three cloud computing service models is shown as horizontal layers via the blue horizontal interoperability points in a stack. The orange vertical interoperability points visualize the vertical interoperability serving the so-called "*verticals"* (Figure 1), such as NATO (public sector) with custom IT services. Subsequently, organizations such as the Dutch military or NATO (public sector) always remain responsible for governance; however, the so-called *verticals* can outsource IT/OT services management (asset-based, IaaS, PaaS, or Saas) to "other participants."

2.4 Challenges for cybersecurity governance

The cybersecurity governance challenges follow from aligning the Dutch military governance directive "Governance of Defence" [16] with the governance layer of the 3-layer cyberspace conceptualization and the governance principles for value creation, risk management, and supervision.

(1) Long-term value creation versus cybersecurity trade-off

The challenge for the BOD executive directors and mandated IT platform service owners is understanding existing and newly upcoming cybersecurity threats and how this affects the value-creation[51] strategy. The *trade-off* between threats and value creation (such as combat power) enabled by IT platform services determines the extent of required prevention and correction controls. Moreover, the *trade-off* and required controls must comply with governmental/self-regulations and, therefore, also determine whether a use case takes off at all.

(2) Compliance management

However, compliance management is challenging for organizations with many decision-makers at different governance levels, as with the Dutch military. See Figure 26 (APPENDIX G) and 2.3.1. Designing and implementing a compliance management system is essential to remain demonstrable in control via continuous security performance monitoring. Demonstrable through reporting the performance to the BOD, mandated owners, and supervisors. Furthermore, governmental/self-regulations enforce transparency about the security of the series of cyber subdomains (Figure 1). The increased cyber security threats require more transparency to gain trust between the actors of the platform organization (a modeled *ecosystem)* [17] and their partners*,* which is necessary to realize benefits. [1]

(3) Risk management considering cascading effects

Nonetheless, managing risks considering cascading effects into adjacent subdomains (see section 2.2.2) to remain in control is challenging. To illustrate the complexity from a governance perspective, Figure **13** (see section 2.3.3) visualizes adjacent subdomains with horizontal and vertical interoperability supporting NATO and partners. Subsequently, IT platform service owners may be unaware of how critical their service is to other services in layers of adjacent subdomains. For example, a security breach may occur in the technical layer of NATO partners due to exploited vulnerabilities in the enlarged attack surface. At the same time, the actual impact (risk) works out in the Dutch military socio-technical layer of cyber activities. However, the Dutch military BOD expects added value in its operational and supporting process domains (owned by process managers at the strategic level). See Table **11**. To remain in control, the challenge for the Dutch military BOD is

[51] Value-creation: expected value creation for the Dutch military core business processes (value chain) enabled by the provided IT platform services . See section 2.3.2.

designing and implementing a Cyber Risk Management system[52] as one of the Integrated Risk Management (IRM[53]) components in consultation with its partners. The operational performance of the security controls is reported to the tactical (mandated IT service owner) and strategic (mandated process domain owner) governance levels for adjustments in the event of non-compliance. See Figure **7**, visualizing the governance direct and control cycle.

(4) Adjustments to stay in control in the event of non-compliance

Nevertheless, robust (long-term) and agile (short-term) decision-making in the event of non-compliance at the strategic, tactical, and operational governance levels is also challenging. In particular, again, for complex organizations such as the Dutch military with typically diverse cultures [52] and the need for innovation for more fighting power over the enemy. [15] In the event of non-compliance, adjustments by the executive director (and mandated owner) require SA and Sensemaking (see section 2.2.2) to manage risks with cascading effects. APPENDIX G visualizes the complex tuning approach using integrated control cycles per governance level (Figure 26) and the escalation steps up to the BOD (non) executive directors (Figure 28).

Having described the cybersecurity governance challenges in this section, now the time has come to zoom in on the *supervision challenges* of cybersecurity governance in the military cyber subdomain.

[52] CRM (Cyber Risk Management) cycle: entails identifying the critical assets, identifying and assessing their risks for the organization as a whole, defining acceptable risk levels (low-hanging fruit first), deciding ways (s) of handling risks, and designing & implementing cyber risk measures in all cyberspace layers, see section 2.2.2.
[53] IRM (Integrated Risk Management): concerns realizing opportunities and managing threats for performing military tasks, (change) goals we want to achieve compliant with legislation and regulations (compliance management), fitting the organization' wide diversity and coherence of the different functional areas/domains and organizational units. [16]

3. Supervision challenges for securing the cyber domain

This chapter discusses the corporate governance challenges for supervising cybersecurity management. The governance challenges for delegated business owners concerning cybersecurity management are identified in the previous chapter.
First, good supervision is defined and why this is essential for securing the corporate cyber subdomain (section 3.1). After examining the objective of corporate cyber security supervision (section 3.2) and its regulatory environment (section 3.3) against the identified corporate governance challenges in the previous chapter (managing long-term value creation and risks by delegated owners), the supervision challenges become apparent (section 3.4). The requirements for the cyber-security supervision model are specified in section 3.5, rounded off with a summary in section 3.6.

3.1 Defining (good) supervision

Classical regulation is often described as a *"Command & Control" (C&C)* approach, a clear fixed standard backed by sanctions. According to (a) classical regulatory theory, regulation consists of three main parts: a norm or standard for complying with regulations, gathering compliance information, and changing behavior in the event of non-compliance. [7]
The first part, the standard or norm, describes the primary target, the different objectives (covering the target), and how to achieve these objectives. It also includes the choice of agents to conduct regulatory activities: a state-based agent or a self-regulatory body. The second part involves how regulators inspect and monitor activities; this requires regulatees (regulated parties) to provide compliance information. Finally, behavior change concerns how rules are complied with and enforced (advice, persuasion, punishment). [7]
On the other hand, variants of classical regulation stem from the assumption that the classical *C&C* regulation approach affects regulatees differently depending on the circumstances. [7] Subsequently, to address these asymmetries, Lodge and Wegrich offer three variants for the classical *C&C* regulation approach.
These variants are architecture[54], market-based[55], and self-regulation, [7] further elaborated within the Dutch military cyberspace context in section 3.3.
Self-regulation means that regulatees develop self-regulatory procedures and policies, commit to them, and also address the more general public (multi) stakeholder policy objectives. The self-regulation approach complements government regulation based on trust between the state-based agency and the regulatees. [7] Trust in the layered infrastructure (by IT platform actors/stakeholders) is a necessary condition for benefits to be realized. [1]

The (b) Dutch Ministry of the Interior and Kingdom Relations defines supervision as (in line with the classical regulatory theory): "*the gathering of information about whether an act or case complies with the requirements set, then form an opinion about it and if necessary intervene.*" [4]

The (c) Dutch Scientific Council for Government Policy (WRR[56]) requests for: "*focusing on the public interests to be served, highlighting and substantiating the societal benefits of supervision about the costs, clarifying the role of supervision in a complex field of influences, and improving the role that supervision plays in reflection and in drawing attention to problems….*" [5]

[54] Architecture regulation: "*determines what people can and cannot do aimed at changing the behavior of users through (secure) design*", [7] for example, speed bumps to prevent speeding.
[55] Market-based regulation: relies on incentives and self-interest to steer behavior. This variant appeals to individual and organizational self-interest to achieve regulatory goals without formal regimes, for example, via subsidies or taxation. [7]
[56] WRR ("Wetenschappelijke Raad voor Regeringsbeleid"): advises the Dutch government by providing evidence-based information on trends and developments that may have a long-term impact on society. It is the Council's duty to point out contradictions and anticipate problems at the earliest possible stage, to identify problems related to major policy issues, and to propose policy alternatives. [5]

In response to this WRR report, the (d) Dutch Cabinet agrees that supervisory bodies must focus on (further) developing this request. Examples are governance-based supervision (see section 2.1) and collaboration among various supervisory bodies. [6]

Regarding governance-based supervision, the (e) Dutch Monitoring Committee states with the Dutch Corporate Governance Code supervision principle: *"The non-executive directors should supervise the policies carried out by the executive directors. In so doing, the non-executive directors should focus on the effectiveness of the company's internal risk management and control systems."* [2]

The (f) Dutch Inspection Council *('Inspectieraad'*) announced, among other things, in its 2018 letter to the Dutch Cabinet regarding the *'Supervision Innovation Program'* for the upcoming years that the main objectives are to operate more data-driven (supported by IT tools) and follow a risk-driven approach, because only then can limited public funds be used as effectively as possible. [53] An advantage of a risk-based strategy is that it is explicit about the inherently limited resources available to supervision. Instead of time-consuming low-level risks, supervision should focus on potentially systematic risks. A risk-based supervision approach prioritizes supervision activity in line with assessing risks that stand in the way of achieving core regulatory objectives. [7]

According to (g) Lodge and Wegrich, good supervision requires performance within the legislative mandate & intent. Following a *"due process"*[57] by providing a means of equality regarding the regulations. Good supervision also reflects the expertise and is *"efficient*[58]*."* [7]

3.2 Objective of good corporate cyber security supervision

By aligning the (a) classical regulation and supervision definition from the (b) Ministry of the Interior and Kingdom Relations *("the gathering of information about whether an act or case complies with the requirements set, then form an opinion about it and if necessary intervene,")* with the opinion of the (c) WRR (i.e., supervision plays a vital role in safeguarding public interests), with the (d) Dutch Cabinet instructions (i.e., governance-based supervision and cooperation of different supervisory bodies), the (e) Dutch monitoring commitee regarding the code's supervison role principle (*"....focus on the effectiveness of the company's internal risk management and control systems"),* and the (f) Inspectieraad intentions (i.e., data-driven, but above all, a risk-driven approach to supervision focussing on systemic (cyber) risks with limited resources for achieving core regulatory objectives), it can be concluded that the objective of (g) good corporate cyber security supervision (i.e., efficient, stays within legislative mandate and intent, follows due process, and reflects expertise) of the security of the Dutch military cyber subdomain is:

> *"To gain mutual trust* in IT platform services by its actors and society through applying a (1-f/g) risk-based approach executed by (2-c/d) cooperating supervisory bodies based on (3-a/b/c) cybersecurity norms for (4-e/f) compliance monitoring, and by (5-a/b) intervention (in the event of non-compliance).*"
>
> ** Trust in the layered infrastructure is a necessary condition for benefits to be realized.* [1]

[57] Due process: follows procedures providing not only predictability but also allows sufficient time & space for consultation and the consideration of particularly affected constituencies; it grants involved parties rights & obligations. [7]

[58] Efficient (good supervision): regulatory procedures are conducted with minimal wastage and prompt, efficiently minimizing the distortion of market transactions and reducing the compliance burden. [7]

3.3 The Dutch military regulatory environment

According to Lessig, four regulation methods apply to cyberspace and the natural world. These methods will be used here to describe the Dutch regularity environment: (1) regulation through network architecture (standards), (2) social norms (ethics), and (3) the market (costs for maintaining parts of the Internet) are explained in subsection 3.3.1, and (4a) government regulation (law) with (4b) additional self-regulation further explained in subsections 3.3.2 and 3.3.3. [54] A summary in subsection 3.3.4 finalizes this section.

3.3.1 Network architecture, social norms, and market regulation aspects

(1) Network architecture

Architecture standardization forums influence the IT (security) architecture. For example, the Enterprise Architecture Civil Service (EAR) [55] deals with the organization (IST and SOLL) of the information provisioning of the Civil Service, under which the Dutch military (for example, shared services). [15] The EAR is the entry point to the agreements and frameworks. The Civil Service Reference Architecture (NORA) [56] is intended as a directing and guiding instrument. It contains frameworks and existing agreements for setting up the information management of the civil service. Creating facilities within those frameworks and agreements ensures that they work well with other facilities and that optimal use is made of existing solutions. NORA offers implementation guidelines concerning security patterns based on standards such as the BIO and ISO. [60] [61] The focus is designing and operating IT (platform) services regarding 13 mandatory and 30 recommended standards established by organizations such as IETF, IEEE, NIST, ISO, NEN, and OASIS. The NATO Interoperability Standards and Profiles (NISP) [51] prescribes the technical standards and profiles to achieve Communications and Information Systems interoperability in support of NATO's missions and operations. Following the Alliance C3 Strategy, all NATO Enterprise entities shall adhere to the NISP mandatory standards and profiles.

(2) Social norms

Social norms set constraints on the regulatory environment, according to Lessig. [58] What is considered appropriate social behavior? The influence of social norms on IT provisioning concerns, for example, the expectation that, nowadays, everybody is reachable via a (personal) device anywhere and anytime. Besides the social norm that everyone is connected, another criterion demands excellent telecommunications connectivity everywhere and all the time. With awareness of the impact of human technology on the natural environment comes the social norm of energy efficiency for new "green" telecommunication systems.

(3) Market

According to Lessig, the market has a regulating effect. [54] Market players united in alliances try to influence IT provisioning from a business perspective, for example, through cost and market price. Market regulation aspects are also part of the Telecom Act (Tw). See the next section, 3.3.2. These aspects concern roaming provisions, net neutrality requirements (e.g., user-experienced data rates), and protecting privacy in electronic communications (e.g., against spam and cookies).

3.3.2 Government regulation (law) and state-based agents (supervision)

This section identifies legal aspects relevant to the supplemental Dutch military cybersecurity self-regulation and its supervision explained in subsection 3.3.3.

(4a-1) State-based agents (supervision)

The Dutch Telecommunications Act (Tw) [57] dedicates chapter 15 to supervision and designates the state-based agents “Agentschap Telecom” (AT), “Data Protection Authority” (AP), and “Authority for

Consumers and Markets" (ACM[59]). These agents play a role in supervising the national legal aspects of cyber security regulations.
AT: The AT is the supervisory body with several objectives, including supervising the usage of frequency space, equipment, and radio equipment specifications on the one hand and supervising authorized tapping and the continuation of public electronic communication networks and public electronic communication services on the other.
ACM: Tw designates ACM as the supervisory authority for market regulation aspects.
AP: The Dutch GDPR Implementing Act, the 'Uitvoeringswet Algemene Verordening Gegevensbescherming' (UAVG), designates only the AP as the supervisory body. The Authority for Personal Data (AP)[60] objective is to supervise compliance regarding the notification of personal data breaches. The Network and Information Systems Security Act (Wbni) [58] designates the state-based agents for DSPs (Digital Service Providers, e.g., cloud computing services) and ESOs (Essential Service Operators). The Wbni assigns the role of CSIRT for ESOs to NCSC (Ministry of Justice and Security) and DSPs to the Ministry of Economic Affairs and Climate Policy. [58] [59]
ILT: The Human Environment and Transport Inspectorate (ILT[61]) supervises providers of essential services (ESOs) that fall under the responsibility of the Ministry of Infrastructure and Water Management, for example, the KMar (at Schiphol).
CTIVD: The Wiv regulates the prior assessment by the Assessment Committee Deployment Competences (TIB[62]) and the supervision afterward by the Intelligence and Security Services Supervisory Committee (CTIVD[63]). [60] The CITV was established based on the Wiv. This committee was installed on 1 July 2003 and is charged with retroactively supervising the actions of the services in implementing the Wiv and the Wvo. However, this only tests for the lawfulness and not for effectiveness. The committee can obtain solicited and unsolicited information and advise the relevant ministers on its findings.

(4a-2) Government regulation (regulation by law)

The Dutch law (legal order) has adopted the European Electronic Communications Code directive (EECC) [61], e-Privacy directive, [62] the General Data Protection regulation (GDPR) [63], and Network and Information Systems Security (NIS/NIS2) directive; [59] [64] these directives and regulation relate to cyber security. The EECC, NIS/NIS2, and current ePrivacy directives are not directly applicable to Dutch law. The EU directives must first be transposed into national law before they are applicable. Unlike the GDPR and the proposed ePrivacy regulations, which are directly applicable in Dutch law after entering into force. [65] The Dutch laws are adopted or transposed from these EU laws.
Tw: The Dutch Telecommunications Act (Tw[64]) is transposed from the EECC and the current ePrivacy Directives. [57]
Wbni: The Dutch Act on Protection of Networks and Information Systems (Wbni[65]) [58] is transposed from the current NIS directive (an update of the current Dutch Wbni is expected based on NIS2).
UAVG: The General Data Protection Regulation Implementation Act (UAVG[66]) [66] adopted the GDPR.
WPG: The GDPR gives Member States considerable flexibility about around thirteen exceptions, but as a law, it is immediately enforceable across the EU from 25 May 2018. One of these exceptions is

[59] ACM: Autoriteit Consument en Markt. [57]
[60] AP: Autoriteit Persoonsgegevens. [57]
[61] ILT (Inspectie Leefomgeving en Transport): supervises providers of essential services (ESOs) that fall under the responsibility of the Ministry of Infrastructure and Water Management. [58]
[62] TIB: Toetsingscommissie Inzet Bemachtheden). [60]
[63] CITV (Commissie Toezicht op de Inlichtingen- en Veiligheidsdien): was established based on the Wiv. [60]
[64] Tw (Telecommunicatie wet): is transposed from the EECC and the current ePrivacy Directives. [57]
[65] Wbni (Wet bescherming netwerken en informatiesystemen): transposed from the NIS directive. [58]
[66] uAVG (Uitvoeringswet Algemene Verordening Gegevensbescherming): adopted the GDPR. [66]

processing personal data to prevent, detect, or prosecute criminal offenses. This 'police data' falls under a separate Police Data Act (WPG[67]). [67] [68]
UAVG: The primary objectives of the UAVG are to prevent and mitigate security breaches, to take the proper organizational and technical precautions to ensure an adequate level of security appropriate to the risk, and to notify a supervisory authority of a security breach likely to result in serious harm. The newest technologies usually lag behind associated standards and regulations since legislative processes might take a long time. A Data Protection Impact Assessment (DPIA) is conducted for specific processes. A DPIA is a process by which the data protection risks of a project are identified and minimized.
Note: Public and military sector regulations (see subsection 3.3.3) prescribe [69] an Information Security Management System (ISMS[68]) and determine whether a DPIA must be performed for a specific process. [68]
WvO: A security investigation, within the meaning of the Dutch Security Investigations Act (Wvo[69]) [70], is an investigation of a person conducted before an employer appoints them to a position of trust. Security investigations in the Netherlands are carried out by the MIVD and the AIVD or on behalf of the latter by the National Police, the Royal Netherlands Marechaussee, and the Security and Protection Service. [70] The WvO is also not directly applicable or transposed from EU law.
WiV: The Intelligence and Security Services Act (Wiv[70]) [60] is a Dutch law (not directly applicable or transposed from EU law) and forms the legal framework for the General Intelligence and Security Service (AIVD[71]) and Military Intelligence and Security Service (MIVD[72]).
In short, the Dutch laws adopted or transposed from EU laws pursue the same general cybersecurity objectives. In general, the EU directives and regulations aim to follow the objectives of preventing and mitigating security breaches and contain a "*duty of care*" that obliges regulated entities to carry out a risk assessment based on which they take appropriate measures (and maintain a record: GDPR Article 30-1 & 32-1). However, the directives do not define risk levels (or thresholds) as to what is appropriate. Other objectives of the EU laws are for regulated parties to notify a supervisory authority of a security breach likely to cause significant damage ("*incident reporting"*), to introduce a more intensive supervisory regime ("*supervision"*), and to contribute to more significant European "*harmonization"* and a *higher level of cyber security* in organizations. [71] [59] [64] [62] APPENDIX K provides an overview of these EU laws.

3.3.3 Self-regulation and supervision

Architecture standardization forums such as EAR, NORA, and NISP influence the network architecture (IT platforms) of organizations, as stated in subsection 3.3.1. [62] [14] These sector-specific civilian standards can fill in Dutch military cybersecurity controls (norms) of regulations. On the other hand, some standards are widely adapted and can be a prerequisite for cooperation within sectors such as the military or sectors, as shown in Figure 1, or even enforced by EU and Dutch law. [72] [73] [74] As mentioned in the previous chapter, the Dutch military has established self-regulation and corporate governance to support the mission, strategy & decision-making

[67] WPG (Wet Politie Gegevens): one of the GDPR exceptions is processing personal data to prevent, detect, or prosecute criminal offenses. This 'police data' falls under a separate Police Data Act (WPG). [67] [68]
[68] ISMS (Information Security Management System): a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's information security to achieve business objectives. It is based upon a risk assessment and the organization's risk acceptance levels designed to treat and manage risks effectively. [113]
[69] Wvo (Wet veiligheidsonderzoeken): regulates a security investigation of a person conducted before an employer appoints them to a position of trust. [70]
[70] Wiv (Wet op de inlichtingen- en veiligheidsdiensten): forms the legal framework for the General Intelligence and Security Service (AIVD) and Military Intelligence and Security Service (MIVD). [60]
[71] AIVD: Algemene Inlichtinen en VeiligheidsDienst.
[72] MIVD: Militaire Inlichtinen en VeiligheidsDienst.

through the “Governance at Defense Directive”. [16] The directive is a form of self-regulation that also specifies the main tasks and responsibilities of the Security Authority (BA): establishing security regulations and internal supervision.

(4b-1) Military cybersecurity regulation

The Dutch military security regulations stem from NATO and the *"Decree Chief Security Officer (CSO) structure civil service 2021”*. [75] [20] An essential objective of the civil service degree and NATO regulations is to formally authorize and approve special information processing *"to ensure an appropriate level of security in view of the interest to be protected."* [20] Through the formal accreditation[73] process, the supervisor (BA/BC) formally grants permission by providing formal approval notes to owners for using IT platform services in which special information is processed. The supervisor (BA/BC) may grant a (Temporal) Approval To Operate (ATO/IATO[74]) after receiving signed compliance statements and reviewing underlying documentation such as technical design, risk assessment, test, audit, and penetration test reports. The owner and IT platform service supplier(s) sign the compliance statements. The *Decree CSO structure civil service* is the umbrella for the: "*State Information Security Regulations (VIR),*" [71] “*State Information Security Special Information 2013”* (VIR-BI), [72] and *“Baseline Information Security Government”* (BIO) Framework. [69] The BIO is based on the widely adopted International Organization for Standardization (ISO) 27001 and 27002 frameworks. [76] [77] The VIR-BI (Article 6-2) prescribes that security is organized based on risk management. [72] The BIO specifies that organizations must register civil service measures that are not (yet) fully complied with, resulting in (temporal) unacceptable risks (this is in line with the GDPR Articles 30-1 and 32-1) following the “*comply or explain principle.”* The BIO also prescribes [69] an Information Security Management System (ISMS[75]) for registering and managing (temporal) unacceptable risks (with cascading effects in adjacent subdomains) in the event of non-compliance (section 2.2.2). The General Security Requirements for Defense Assignments (ABDO[76]) applies to military partners in the private sector. Following ABDO, accountability for security via ABDO authorization is a contract condition for procuring services that process confidential information & support vital processes. [78] The technical and implementation directive for CIS Security[77] provides the minimum set of security requirements to be applied for the protection of NATO classified and non-classified information and the handling of CIS. [79] The NATO and national Security Accreditation Authority (SAA) shall use the directive. The SAA is responsible for approving a (CIS) system to store, process, or transmit NATO classified information up to a defined classification level (including, where appropriate, special categories) in its operational environment. [75]

(4b-2) Supervisory authority

The Dutch military established regulations to support the mission, strategy & decision-making through the Governance at Defense Directive, a form of self-regulation. Regardless of the organizational suspension, the Dutch military supervisors[78] have an independent position under the General Defence Organization Decree [80] and direct access to the SG (see 2.3.1). [16]

---

[73] Accreditation: formal authorization and approval of special-information processing (article 1). [20]

[74] (Temporal) Approval To Operate (ATO/IATO): issued every three year by BC/BA (earlier for intervention). [20]

[75] ISMS (Information Security Management System): a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization’s information security to achieve business objectives. It is based upon a risk assessment and the organization’s risk acceptance levels designed to treat and manage risks effectively. [113]

[76] ABDO (Algemene Beveiligingseisen voor Defensieopdrachten): private sector companies that handle special information must comply with the security requirements. [78]

[77] NATO AC/322-D/0048-REV3 (INV): CIS Technical and implementation directive. [79]

[78] Dutch military supervisors: Inspecteur-Generaal Veiligheid (IGV), Directeur Militaire Luchtvaart Autoriteit (MLA), Commandant Korps Militaire Controleurs Gevaarlijke Stoffen (KMCGS), Inspecteur Militaire Gezondheidszorg (IMG), Functionaris Gegevensbescherming (FG) en Beveiligingsautoriteit (BA). [80]

A CSO structure is set up for the civil service and laid down in a formal decree to support and advise the (deputy) Secretary-General (SG) of the various government departments in the field of integrated security. The Ministry of the Interior and Kingdom Relations (BZK) is responsible for the CSO structure and stems from the 'Decree CSO structure civil service 2021' [20] consisting of:

- Governmental CSO (BVA Rijk);
- Departmental CSO (BVA 'Beveiligingsambtenaar');
- Organizational CSO (BVC 'Beveiligingscoordinator').

The SG authorizes the BVA for the Security Accreditation Authority (SAA[79]) role. [20] To prevent conflicts about independence and interests, the integral assessment and testing of the accreditation process lie with the departmental BVA. The BVA can be mandated to grant prior permission on behalf of the Secretary-General to process information in national systems. Accreditation is:

"Formal authorization and approval of special-information[80] *processing, taking the operational environment into account. It is a form of (pre-)supervision to ensure an appropriate level of security given the interest to be protected."* (article 1) [20]

The Dutch military SG has mandated the departmental CSO and SAA roles to the security Authority (BA), the organizational CSO role to the Beveiligingscoordinator (BC), and the Data Protection Officer (DPO) role to the "*Functionaris Gegevensbescherming" (FG).* The DPO role within organizations supports the Authority Personal data (AP) charged with supervising compliance regarding the notification of personal data breaches (GDPR). [63] The Dutch military SG has mandated the Military National Security Authority (NSA) task of NATO and EU to the Security Authority (BA). The NSA is responsible for securing classified information from other international partnerships & treaties and conducting periodic inspections. [16]

3.3.4 Summary of subsection 3.3

Four forms of regulation influence cyberspace and the natural world: regulation through architecture (such as software code), society/ethics (what is considered appropriate social behavior?), the market (costs associated with maintaining parts of the Internet), and (inter) national law (and supplemental self-regulations). Generally, the (inter)national law aims to prevent and mitigate security breaches and contains a *duty of care* that obliges regulated entities to carry out a risk assessment. However, these provisions do not define low, medium, or high-risk levels (with adequate controls). Other objectives are to oblige regulated entities for incident reporting, introduce a more intensive supervision regime, and contribute to more significant harmonization and a higher level of cyber security in organizations.
The Dutch Telecommunications Act (Tw) appoints the authorities "Agentschap Telecom" (AT), "Data Protection Authority" (AP), and "Authority for Consumers and Markets" (ACM) to play a role in supervising the cyber security objectives of the (inter) national laws. The Network and Information Security Act (Wbni) designates the state-based agents for Digital Service Providers (NCSC/CSIRT) and Essential Service Operators (ILT). The Intelligence Supervisory Committee (CTIVD) is charged with retroactively supervising the Intelligence Services in implementing the Intelligence and Security Act (Wiv) and the Security Investigations Act (Wvo).

The supplemental Dutch military (cyber) security regulations stem from the decree Chief Security Officer (CSO) structure civil service (2021) and NATO. An essential supervision objective of the civil

[79] SAA (Security Accreditation Authority): see EU, IA Security Guidelines on CIS Security Accreditation, IASG 1-01, 22 and 24 [114], NAVO, Guidelines for the security accreditation of communication and information systems (CIS), AC/35-D/1021-REV3, Section IV.1.11, [79] VIR-BI, artikel 3 Beveiligingsbeleid. [115]
[80] Special information: information where access by unauthorized persons can have adverse consequences for the interests of the State, its allies, or one or more ministries. [20] [115]

service decree and NATO regulations is the formal approval to use IT platform services for special information processing "*to ensure an appropriate level of security given the interest to be protected*." The civil service regulation prescribes that security accountability is based on “comply or explain,” registration of non-compliances, and security is organized based on risk management. The Dutch military Secretary General (SG) has mandated the civil service departmental supervisor CSO and Security Accreditation Authority (SAA) roles to the BA, the organizational CSO role to the BC, and the Data Protection Officer (DPO) role to the “Functionaris Gegevensbescherming” (FG). The SG has mandated the NATO and EU National Security Authority (NSA) role also to the BA.

3.4 Challenges for corporate cyber security supervision

Following the Hevner design science methodology (see section 1.3), chapter two describes the “problem domain” and identifies governance challenges from aligning the Dutch military governance directive “Governance of Defence” [16] with the governance layer of the 3-layer cyberspace conceptualization and the governance principles for value creation, risk management, and supervision. Chapter three analyzes the “problem domain” based on desk research (section 3.1 a-g) and reports of semi-structured interviews for identifying challenges for supervising cybersecurity management in the Dutch military domain and adjacent subdomains. See also APPENDIX A.

(1) Risk-based supervision approach (see also 3.2 f-g)

Accounting for systematic risks with cascading effects into adjacent subdomains (2.4-3) supporting units outside the supervisor regulatory areas is challenging for the current risk-based supervision approach. The legal (inter)national provisions oblige regulated entities to carry out a risk assessment but do not define low, medium, or high-risk levels (3.3.2) with *adequate cybersecurity controls* that all *cooperating supervisor bodies* (3.4-2) must consider. In addition, supplemental organizational self-regulation, such as from the Dutch military units and civil service partners, usually relates to reliability (3.3.3).

Actually, organizations should consider reliability with the associated risk levels and *adequate cybersecurity controls* (3.4-3) of the underlying IT platform services and determine whether a use case takes off (2.4-1). However, this is often time-consuming and requires specialized technical knowledge of the IT service suppliers, which is not always available for all supervisors. Furthermore, given the complexity of the Dutch military governance model for decision-making (on three levels), it can be concluded that risk-based supervision of compliance and risk management (3.4-4) that takes cascading effects into account is challenging.

(2) Cooperating supervisory bodies (see also 3.2-c-d)

The legal provisions aim to introduce a more intensive supervision regime. However, legal provisions do not define low, medium, or high-risk levels with *adequate cybersecurity controls* that organizational units of adjacent subdomains must consider, challenging the cooperation between their supervisors. In addition, supplemental self-regulation often requires management reporting on reliability/security performance (2.4-2) with associated risk levels and associated *adequate cybersecurity controls* (3.4.3).

Nevertheless, joint supervision is challenging when the reporting on the security performance of IT platform services is based on an ineffective *compliance and risk management system* (3.4.4).

(3) Adequate cybersecurity controls (see also 3-a-b-c)

Challenging is the application of mutually accepted *control frameworks*[81], which concerns safeguarding general public policy objectives and (timely) reducing the gap with the latest technologies and government regulations. [81] [78] *Systemic risks* with cascading effects into

[81] Control frameworks: the Dutch military is bound by civil service (BIO) and NATO/EU frameworks. The BIO framework is high over and does not consider state actor threats, unlike the NATO/EU frameworks.

adjacent subdomains might trigger widespread failures and adverse effects in diverse supported organizational units and process domains (value chain). Therefore, the security objectives may differ for cybersecurity control frameworks. For example, the security objectives for the medical process domain may differ from the military operational or public sector process domain regarding privacy versus military intelligence & security aspects.

(4) Information collection and monitoring compliance (see also 3.2-e-f)

Maintaining an overview and situational awareness by the supervisor becomes challenging when collecting information and monitoring compliance (2.4-2) involves risks with cascading effects in adjacent subdomains outside the regulatory area. For example, when adjacent subdomains support (inter) national partners, including IT service suppliers, offering on-premise and off-premise managed services. [37]

(5) Intervening in the event of non-compliance (see also 3.2-a-b)

When forming an opinion and possibly intervening (2.4-4), the risk of inconsistency between supervisory regimes may arise. Moreover, user perception of risk is challenging and is likely to differ from the rational opinion of experts. [7]

3.5 Putting it all together: requirements for the cybersecurity supervision model

Based on the identified challenges in the previous section following the design science methodology, this section presents the design requirements or the "possible solution" or "artifact": the integrated cyber security supervision model. The execution of the engineering cycle, depicted in Figure 5, results in identified design requirements.

To ensure trust with stakeholders of the "*supervised parties*[82]*"* in the cybersecurity (end-to-end) in IT platform services, the requirements for an integrated cybersecurity supervision model for the Dutch military domain are:

1. Implement a risk-based approach considering systematic risks with cascading effects into adjacent subdomains that support Dutch military and partner units;
2. Cooperation between supervisors of adjacent subdomains that support Dutch military and partner units;
3. Application of mutually accepted and up-to-date cybersecurity control frameworks;
4. Collect information from supervisors from the growing number of Dutch military and partner units to create situational awareness. Units with, for example, IT service contractors and sub-contractors. Supervisors address this by focusing on the effective operation of a risk management and control system and their mutual coordination in monitoring compliance. Therefore, supervisors must focus on systemic risks (and some "*random security tests*[83]*"*) instead of time-consuming low-level risks (treatment of symptoms);
5. Intervene in the event of non-compliance, considering systemic risks (with cascading effects) and using up-to-date controls accepted by supervisors for adjacent subdomains supporting the diverse Dutch military and partner units.

[82] Supervised party (regulatee): organization, person, IT (platform) owner, group, or other body on whose behalf a risk analysis is conducted.

[83] Random security tests: desk research (setup), acceptance tests (existence), or penetration tests (exploitation).

4. Building the cybersecurity supervision model

This chapter aims to design and build the cybersecurity supervision model (artifact). Section 4.1 gives substance to the first model design requirement and focuses on the risk-based supervision approach. Section 4.2 focuses on the interaction between supervisors by implementing the remaining design requirements, and section 4.3 verifies the model finalized by a summary in section 4.4.

4.1 Risk-based supervision approach to cybersecurity

This section provides substance to the first requirement (derived in the previous chapter) for an integrated cybersecurity supervision model for the Dutch military domain. The first requirement is examined from a risk management perspective (section 2.2.2) in light of the identified supervision challenges (section 3.4).

4.1.1 Implementation steps

The ISO/IEC 31010 [82] is a frequently used framework for several risk management methodologies. APPENDIX L (Figure 29) depicts the iterative steps.

The "*Bowtie*" model, explained in section 2.2.2, is an example methodology that fits the iterative steps of the ISO risk management framework. The *Bowtie* steps model the risk-based approach:

(a) Establishing the context;
(b) Identifying the critical assets (crown jewels);
(c) Identifying and assessing the asset risks;
(d) Defining acceptable risk levels (low-hanging fruit first) for the Dutch military and partner units;
(e) Deciding ways of dealing with risks (accepting, avoiding, mitigating, transferring);
(f) Designing and implementing risk controls (measures) in all cyberspace layers;
(g) Monitoring the effectiveness of the implemented controls (cyber Situational Awareness and Sensemaking).

4.1.2 Implementing the risk-based approach

The first design requirement for an integrated CyberSecurity (CS) supervision model for the Dutch military domain is implementing a risk-based approach considering cascading effects into adjacent subdomains supporting Dutch military and partner units (to ensure mutual trust).

(a) Context

With the risk-based approach, the supervisor aims to achieve regulatory objectives within the (Dutch military) *boundary conditions* as effectively as possible**.** The objective is to identify, assess, and analyze risks arising from breaches of (trust in the) security in the (multi-stakeholder[84]) IT platform services within the Dutch military user context. As described in section 2.2.1*, boundary conditions* include available resources, time frame, the legislative (and supplemental self-regulation) mandate, and intent (3.2 f-g). [7] The provisioning of IT (platform) services is modeled following the *conceptualized cyberspace layers.* [3] Cybersecurity controls (norms) are then proposed to the Dutch military supervisory body within an appropriate risk treatment strategy from a governance perspective. Consideration of failing controls resulting in security breaches is required. In this scenario, breaches in the technical layer have an actual impact (risks) on the socio-technical layer of cyber activities). [3]

[84] Multi-stakeholders: IT platform service suppliers, owners, producers and consumers. [17] General public (multi) stakeholder policy objectives of these regulatees are addressed by self-developed regulations. [7]

The integrated CS supervision model layers

The supervision and owner layers represent the governance layer. From the supervision layer, the supervisors oversee the controls implemented in the socio-technical and technical layers and report to the BOD and supervisory bodies of Dutch military partners (supported by adjacent subdomains). Section 4.2 (design requirement 4) discusses the information flows toward the BOD, partners, and between the supervisor, owner, socio-technical, and technical layers and how this relates to the Plan, Do, Check, and Act cycle. The mandated supervisor focuses on the effectiveness of the risk management and control systems part of the owner layer. Effectiveness concerns the security performance of the implemented controls over which the mandated owner is responsible.

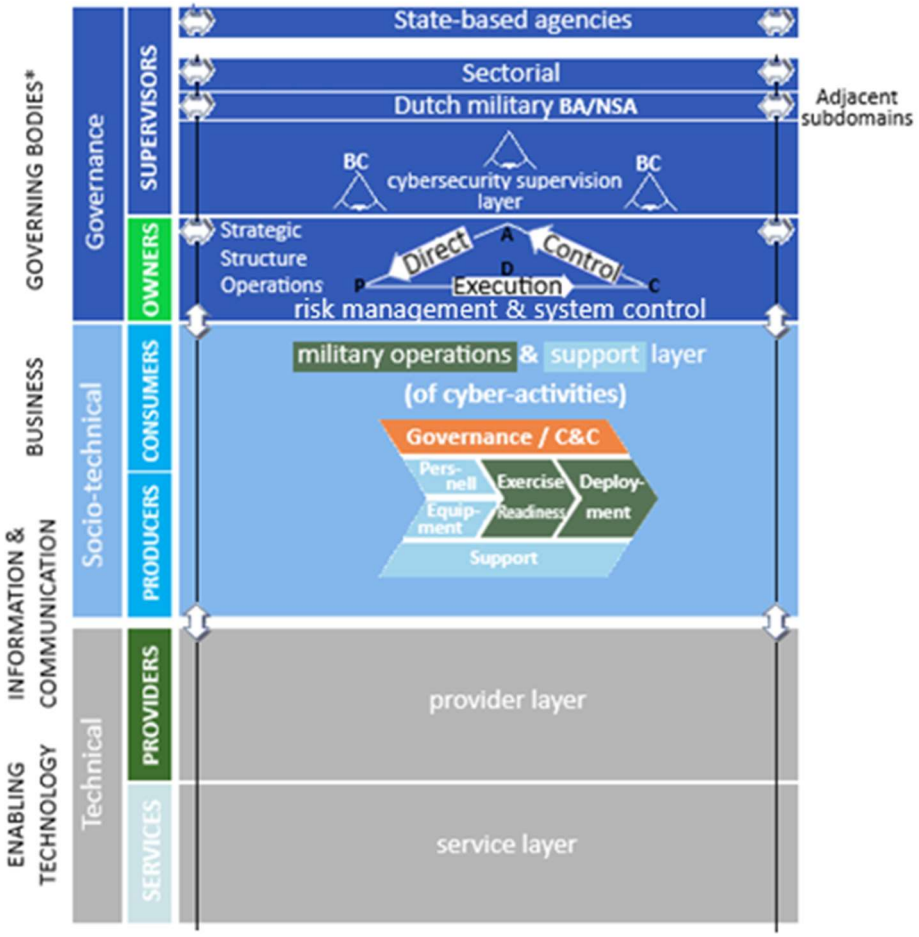
The owner layer comprises the IT platform owner roles at the strategic, structure, and operational levels inspired by "A generic framework for the "Business-IT Relationship" (Figure 3) and the "Governance Direct Control cycle" *(*Figure 7). Following the directive "Governance at Defense Directive," [16] the Dutch military units should have a compliance management system, one of the Integrated Risk Management (IRM) components in place.

The military operations/support layer represents the socio-technical layer, where IT platform users (producers and consumers) can enjoy the provided IT application services and create value (see value chain in Figure 9, section 2.3.2) for each other. [17] Human actors, such as the Dutch military staff, execute or initiate cyber activities. However, some cyber activities (such as in OT) are fully automated.

The IT platform provider and Service Building Block (SBB) layers equal the technical layer. The provider layer comprises the network telecom equipment for providing the SBBs and the end-to-end management of the provided SBBs. The IT platform service provider performs (and reports) according to the agreed (with the owner) security/quality performance related to the aggregated critical assets (IT services that process information). The emphasis is on the performance of implemented controls for mitigating risks regarding the typical information security objectives for ensuring Confidentiality, Integrity, and Availability (CIA).

The SBB layer includes asset and cloud-based solutions with virtualized network functions based on innovative civilian technologies. See Figure 12, section 2.3.3, or Figure 29; APPENDIX J.

Figure 14 depicts the CS supervision model layers for the Dutch military. The "*adjacent subdomains*" of the Dutch military are part of the public and private sectors, for example, subdomains owned by NATO, the Dutch Ministry of the Interior & Kingdom Relations, or Microsoft.



* One-tier BOD: composed of (non) executive directors represented by the owner and supervisor roles

FIGURE 14 MODELED IT PLATFORM CYBERSPACE LAYERS BASED ON THE CONCEPTUAL CYBERSPACE OF VAN DEN BERG ET AL. [17] [3] [16] [19]

Mapping the approach to the modeled IT platform cyberspace layers

The overall goal of the supervisory bodies is to ensure trust among their stakeholders following the iterative risk management steps within *boundary conditions* such as (inter)national provisions (jurisdiction) and the supplemental regulatory area of the supervisor.

After establishing the (a) context, the regulatees (with the owners responsible) account to the supervisors for the (b) identified critical assets (crown jewels) and (c) associated risks.

Note 1: the local or central IT platform service supervisor (BC or BA) may be unaware of the criticality of IT services in layers of adjacent subdomains (or vice versa). The current risk-based approach of the supervisor does not consider risks with cascading effects.

For defining (d) acceptable risk levels, it is essential to consider cascading effects into adjacent subdomain layers (challenge 3.4-1) of the modeled IT platform (Figure 14) to ensure trust in end-to-end security. Cooperation between the supervisors (challenge 3.4-2) of the Dutch military and partner units is essential for defining acceptable risk levels for the supporting adjacent subdomains. In the next step, the supervisor can intervene in the event of non-compliance with the regulations by issuing a formal Interim Approval To Operate (IATO) or rejection (section 3.3.3). In this scenario, the supervisor demands (e) risk treatment by regulatees according to their regulations. Subsequently,

the owner(s) is/are ultimately responsible for (f) designing and implementing controls in relevant layers to mitigate risks to acceptable levels. Finally, the supervisor(s) (g) monitor the effectiveness of the controls to obtain cyber SA and Sensemaking. The iterative steps are triggered again in the event of non-compliance. Again, a critical boundary condition is cooperation between the supervisors of adjacent subdomains.

Note 2: in the event of non-compliance, the supervisors (supervision layer) demand that the regulatees (IT platform actors), with the owners responsible (owner layer), implement adequate controls for mitigating (temporal) unacceptable risks regarding the identified critical assets.
The critical assets for the operation/support layer are the cyber activities executed or initiated by users (cyber processes, such as in OT, are fully automated). The risks concern the lack of secure behavior of human actors (or non-human actors).
The information processed by the provided IT services is critical for the provider and service layers. The controls for the provider and service layers aim to mitigate risks related to the well-known information security/reliability objectives for confidentiality, integrity, and availability. Finally, the IT service provider and the owner agree on service levels regarding the reliability/security performance of the sum of the IT services provided, including well-defined boundary conditions for usage.

(b) Critical assets

From the perspective of the Dutch military CS supervision layer, to ensure trust, the owner is ultimately responsible for convincing the supervisor of secure critical assets[85] as part of the CS supervision military operations/support, provider, and service layers shown in Figure 14.

First, the critical asset is trust in the security of the owner/management layer. The owner identifies and registers the crown jewels in terms of military operations (see Figure 9) and related critical cyber activities. Next, from these critical cyber activities, follow the identification and registration of provider and service layer assets in terms of critical IT services (processing critical information). The owner then decides and registers the risk handling (risk management and control system).

Subsequently, from the supervisor's perspective, the critical asset is trust in the security of the operation/support layer of cyber activities, the provided application services, such as C&C, Situational Awareness, O&T, medical, and Intelligence services, as shown in Figure 4.

Analogously, from the supervisor's perspective, the critical asset for the provider layer is the trust in the security of the network/communication provider (composed of, for example, communications equipment, cables, or satellite systems). Finally, the critical asset for the IT service layer is trust in the security of the cloud-based/virtualized IT services such as APIs, Community Of Interest (COI), and end-user (commercial) services. See Figure 13 (section 2.3.3) and Figure 29 (APPENDIX J).

(c) Risk Identification

The objective is to identify the associated risks (with cascading effects) for the (b) critical assets of the CS supervision model layers.

(1) Actors

The IT platform organization actors, shown in Figure 2, represent the actors of the regulatees (supervised parties) with the owner responsible. Figure 3 shows the business - IT relationship for the IT platform actors at the strategic, tactical, and operational levels [28] mapped to the conceptualized cyberspace layers. The Dutch military cooperates with partners in, for example, the insurance,

[85] Asset: ISO defines an asset as an item, thing, or entity with potential or actual value to an organization. Hence, an asset for which a party requires protection. [88]

financial, IT/OT/Telecom, or government (public) sectors. See Figure 1 for other examples. The relation between the supervised (supervision layer) decision-makers (owner layer) for governing the business (operation/support layer) and ICT (supplier and service layers) actors at the strategic, tactical, and operational governance levels are visualized in Figure 21 and Figure 20 (APPENDIX B).

(2) Vulnerabilities

Vulnerabilities[86] are viewed from the supervisor layer, overseeing the remaining layers of the modeled IT platform (shown in Figure 14). Trust in (the security of) the owner layer can be weak If proper cybersecurity skills training, SA, and sensemaking (see section 2.2.2) are missing from agile/robust decision-making regarding risk management. The operations/support layer can be vulnerable due to flaws in the provided application or usage outside the agreed boundary conditions regarding the Dutch military Code of Conduct for E-mail and Internet Facilities. [83] [84] For example, Dutch military staff should choose the proper IT (platform service) means for transmitting classified information/marked documents and, ideally, are unknowingly cybersecurity-skilled. In the user scenario shown in Figure 10, lacking training for these cybersecurity skills may result in leaking state secret battlefield information during critical military operations. The vulnerabilities in the provider layer relate to flaws in the equipment/assets of IT or telecom network providers. For example, malicious actors exploit weak encryption of radio signals by eavesdropping. The vulnerabilities of the service layer include flaws in cloud-based / virtualization services such as API services, Identity Access Management (IAM), or (virtualized) firewall services. An example is a software bug exploited by a virus.

(3) Threat events and (4) threat sources

Again, viewed from the supervision layer, specific threats[87] such as social engineering attacks may target the organizational owner layer (military owner actors) and the operational/support layer (military user actors). For example, malicious state actor threat sources exploit the *(2) vulnerabilities* regarding lack of training in cybersecurity skills. Therefore, trust in (the security of) the owner and operational/support layers can be weak when executing social engineering attacks. Threat sources (such as hackers) may also attack the operational/support layer by exploiting vulnerabilities in provided application services through spoofing/identity theft.

On the other hand, the 'Man in the Middle' (MitM) attack aims to exploit vulnerabilities in, for example, cables, satellites, or telecom equipment part of the provider layer. Subsequently, the impact (risks) work out on the operations/support layer of cyber activities.

The same goes for attacks aimed at exploiting vulnerabilities in the service layer (such as API, COI, or IAM services), causing failures in the service Layer and impacting the provider layer on top. A threat may come from an intentional security event by malicious state, criminal, or terrorist threat sources or an unintentional safety event (natural disaster or power outage).

APPENDIX M presents an overview of adversarial, structural, or environmental threat sources and events in Table 12 and Table **13**, taken from the NIST "Guide for Conducting Risk Assessments." [85]

[86] Vulnerabilities: ISO defines a vulnerability as a weakness in a (critical) asset or a sum of assets that one or more threats can exploit, and (proactive) steps should be taken to address it. [88]

[87] Threats: ISO defines a threat as a potential cause for an incident that may harm organizations, assets, or cloud-based services and cannot be controlled (generally). [88]

(5) Consequences

Ultimately, the consequence is a breached trust of the IT platform *(1) actors* in the security of the sum of the IT platform services provided. However, the consequences may differ per layer of the IT platform model depicted in Figure 14. Seen from the CS supervision layer, the integrated (end-to-end multi-stakeholder) CS supervision IT platform model to ensure mutual trust within the *(a) context*/boundary conditions is the sum of:

(b) Critical assets: trust in (the security of) the owner/management (identification/registration of critical assets and risk handling decisions), operation/support (critical cyber activities), provider (security performance), and service (critical processed information) layers;

(c1) Actors: the IT platform mandated owners, users, providers, BOD, MOD, government, and finally, society as a whole (multi-stakeholder);

(c2) Vulnerabilities: exploited (such as by social engineering attack) weakness in trust of (the security of) the owner/management, operation/support (such as logistics, intel, H&R, C&C cyber activities) layers or exploited (such as by Man in the Middle attack) weakness in trust of (the security of) provider (performance via network/communication equipment such as satellites, antennas, routers, or cables), or service (performance of asset/cloud-based) layers;

(c3) Threat events: attack (such as by social engineering) resulting in a breach of trust in the (security of) the owner (risk management and control system), operation/support (cyber activities), or attack (such as by Man in the Middle) resulting in a breach of trust in the provider (performance of communication/network provider equipment), and of services (performance of asset/cloud-based) layers;

(c4) Threat sources: the adversarial (such as individual, group, or nation-state) and non-adversarial (such as equipment failure) malicious actors;

(c5) Consequences: loss of trust may result in reputation damage for the government, MOD, the BOD (non) executive directors, mandated supervisors, mandated owners, users (consumers and producers), or providers. Other consequences are reduced operational Dutch military fighting power, public unrest, economic damage, or financial claims; lower security performance (confidentiality, integrity, availability, and continuity) of the provisioning of services.

(d) Defining acceptable impact/risk levels

Risk[88] is the product of the probability of an (inter) dependent incident and its impact (see Figure 8). The probability relates to the *(d1) likelihood* of a threat and the *(d2) ease of exploitation* of a vulnerability. [86] Viewed from the supervision layer, for the Dutch military integral (end-to-end multi-stakeholder) CS supervision IT platform model, the acceptable true *(d3) impact/(d4)* risk level (of trust) of cyber security is defined for the:

1) Owner and operation/support layers regarding exploited vulnerabilities in the:
    a. behavior (critical cyber activities) of the IT platform actors (owner, user, and supplier roles);
    b. provider critical equipment;
2) Provider layer regarding exploited vulnerabilities in the provided critical IT services;
3) Service layer regarding exploited vulnerabilities in the critical asset/cloud-based Service Building Blocks.

(1) Likelihood & (2) ease of exploitation rating

The likelihood of the occurrence of a cyber (or threat) incident and the ease of exploiting a vulnerability is rated Low, Medium, or High. Table 14 and Table 15 (APPENDIX N) are rating examples from the NIST "Risk Management Guide for Information Technology Systems." [86]

[88] Risk (ISO): the effect of uncertainty on objectives, usually expressed in terms of risk sources, potential events, their consequences, and their likelihood. [34]

(3) Impact rating with predefined TBB categories

The Dutch military rates the impact of *(b) critical assets* based on four categories of interests to be protected (TBB[89]). The potential impact of a threat event is valued in terms of replacement or reconstruction costs (in other words, quantitative measurements).

Table **16** (APPENDIX O) presents a NIST example for rating the potential impact on operation/support processes based on unauthorized disclosure (confidentiality), modification (integrity) of information, unavailability of information (during different periods), and destruction. The potential impact results of exploited vulnerabilities in:

a. the behavior of actors as part of the owner and operation/support layers of critical cyber activities (for example, proper user handling regarding USB sticks or email/internet);
b. the IT services comprising asset and cloud-based Service Building Blocks as part of the supplier and service layers.

Based on interviews with selected business managers (the IT service and process owners), the business impact is rated Low, Medium, or High for the security objectives, confidentiality, integrity, and availability (versus business continuity). The rating uses qualitative measures such as limited, serious, severe, or catastrophic and must occur within the context/agreed organizational user conditions. Therefore, the NIST rating is refined for each security objective using impact guidelines covering issues typical in the Dutch military (a) context. The impact guidelines cover issues such as personal safety, personal information/privacy, law enforcement, commercial/economic interests, financial loss/disruption of activities, public order, business policy and operations, and loss of goodwill. The highest-rated guideline for each security objective determines the final CIA level, as shown in Table **2**.

	Confidentiality	Integrity	Availability
CIA level (for each security objective, the highest impact guideline rating)	L	H	M

TABLE 2 EXAMPLE CIA LEVEL FOR IT PLATFORM SERVICES: USING THE HIGHEST IMPACT RATING FOR EACH CIA LEVEL.

Finally, the IT platform service TBB category follows from Table 3. The method of transposing the CIA level to a TBB category can be traced back to using the CRAMM tool/methodology in the past. [87]

Old	New	TBB	Old	New	TBB	Old	New	TBB
LLL	**LLL**	4	LML	**LMH**	3	LHL	**LHH**	1 or 2*
MLL	**MLL**	3	MML	**MMH**	3	MHL	**MHH**	1 or 2*
HLL	**HLH**	3	HML	**HMH**	2	HHL	**HHH**	1 or 2*
LLM	**LLH**	4	LMM	**LMH**	3	LHM	**LHH**	1 or 2*
MLM	**MLH**	3	MMM	**MMH**	3	MHM	**MHH**	1 or 2*
HLM	**HLH**	3	HMM	**HMH**	2	HHM	**HHH**	1 or 2*
LLH	**LLH**	4	LMH	**LMH**	3	LHH	**LHH**	1 or 2*
MLH	**MLH**	3	MMH	**MMH**	3	MHH	**MHH**	1 or 2*
HLH	**HLH**	3	HMH	**HMH**	2	HHH	**HHH**	1 or 2*

TABLE 3 CIA LEVEL CONVERSION TO TBB CATEGORIES TBB1[90], TBB2[91], TBB3, AND TBB4

(4) Risk levels

The risk evaluation scores follow from the matrix illustrated in Table 4 when matching the TBB impact category (or asset value) against the threat and vulnerability exploitation ratings. Matching via the matrix provides the risk score for each combination on a scale of 0 to 8. The matrix and rating values are taken from the ISO 27005 standard [88] as an example.

[89] Te Beschermen Belang (TBB): four pre-defined categories of interests to be protected alligned with the Dutch military regulations for the compliance management system, one of the IRM components. [16]
[90] TBB category 1: classification when confidentiality of information is classified: “Top Secret”.
[91] TBB category 2: classification when confidentiality of information is classified: “Secret”.

Likelihood of threat occurrence		Low			Medium			High		
Ease of exploitation		L	M	H	L	M	H	L	M	H
TBB category for the *(b) critical asset*	0	0	1	2	1	2	3	2	3	4
	TBB4	1	2	3	2	3	4	3	4	5
	TBB3	2	3	4	3	4	5	4	5	6
	TBB2	3	4	5	4	5	6	5	6	7
	TBB1	4	5	6	5	6	7	6	7	8

TABLE 4 MEASURE OF RISK ISO 27005 TABLE E.1 [88]

The TBB category for an identified critical asset determines the appropriate row in the matrix of Table 4, and the "Likelihood of threat occurrence" and "Ease of exploitation" of a vulnerability determine the appropriate column. For example, if the asset category is TBB2, the threat likelihood is "Medium," and the ease of exploration of a vulnerability is "Medium," then the "Measure of risk" is 5. Next, the "Measure of risk" level is rated Low, Medium, or High, as depicted by the different colors in Table 4: Low 0-2 (green), Medium 3 – 5 (yellow), and High 6 – 8 (red). For the above example, the "Measure of risk" is 5. Subsequently, the risk level is rated Medium.

The relevant threats and related vulnerabilities are considered for each critical asset. Based on the potential impact scenarios (impact guidelines), there is no risk where there is a vulnerability without a corresponding threat or vice versa. However, caution should be exercised if this circumstance changes. The timeframe over which the asset has value or interest to be protected (TBB category) should be identified to assess the likelihood of threat occurrence. [88]

Example risk assessment result

Table **5** shows the cyber risk assessment result of the threat event that exploits (c2) vulnerabilities to breach the trust in the behavior of (c1) owners as part of the owner layer of *(b) critical cyber activities*. The threat event is viewed from the supervision layer depicted in Figure 14. The threat event is (c3-4) the breach of trust in the security of the owner layer due to improper risk management, resulting in high risks in the operation/support layer and inadequate agreed service levels for the supplier for IT services. Subsequently, this may result in disruptions in, for example, the service layer. The (c1) actor column indicates relevant actors-/stakeholders for the interview session for identifying the impact rating with predefined TBB categories. All relevant actors/stakeholders must be involved in establishing the correct dependencies of the layers of the integrated (multi-stakeholder end-to-end) CS supervision model to ensure mutual trust.

Asset (b)	Actors (c1)	Vulne-rabilities (c2)	Threat event (c3-4)	Likelihood threat (d1)	Ease of exploitation (d2)	Potential Impact (d3)	Risk level (Table 4) (d4)
Trust in the security of the owner layer	IT Platform owner (**Fout! Verwijzingsbron niet gevonden.**).	Weaknesses in the training of cyber security skills.	Breach of trust in the security of the owner layer due to improper risk management resulting in high risks in the operation/support layer	**M**	**M**	**TBB2**	**M (5)**

TABLE 5 EXAMPLE OF A RISK ASSESSMENT RESULT

Other examples of risk assessments may start (bottom-up) with a breach of trust in the security of the service layer, with the actual impact (risks) working out in the operation/support layer of cyber activities. Next, the owner should execute risk management, considering cascading effects.

(e) Risk treatment

The supervisors can then intervene in the event of non-compliance within their regulatory areas. In this scenario, the supervisor demands risk treatment by its regulatees, with the owner responsible for following regulations. According to the ISO 27005 standard, [87] there are four risk treatment strategies:

1. Risk-retention: accept or tolerate the consequences of the informed decision;
2. Risk-sharing or transfer: shift the liability (partially or entirely) to another entity;
3. Risk modification: mitigate the risk to acceptable risk levels by implementing controls;
4. Risk avoidance: refraining from certain activities to eliminate risk.

Table 6 matches the four risk treatment strategies to the risk score for all possible combinations.

Likelihood of Occurrence Threat		Low			Medium			High		
Ease of Exploitation		L	M	H	L	M	H	L	M	H
TBB category (asset operations/ support Value)	0	0	1	2	1	2	3	2	3	4
	TBB4	1	2	3	2	3	4	3	4	5
	TBB3	2	3	4	3	4	5	4	5	6
	TBB2	3	4	5	4	5	6	5	6	7
	TBB1	4	5	6	5	6	7	6	7	8

TABLE 6 RISK TREATMENT STRATEGIES PLOTTED TO RISK SCORES

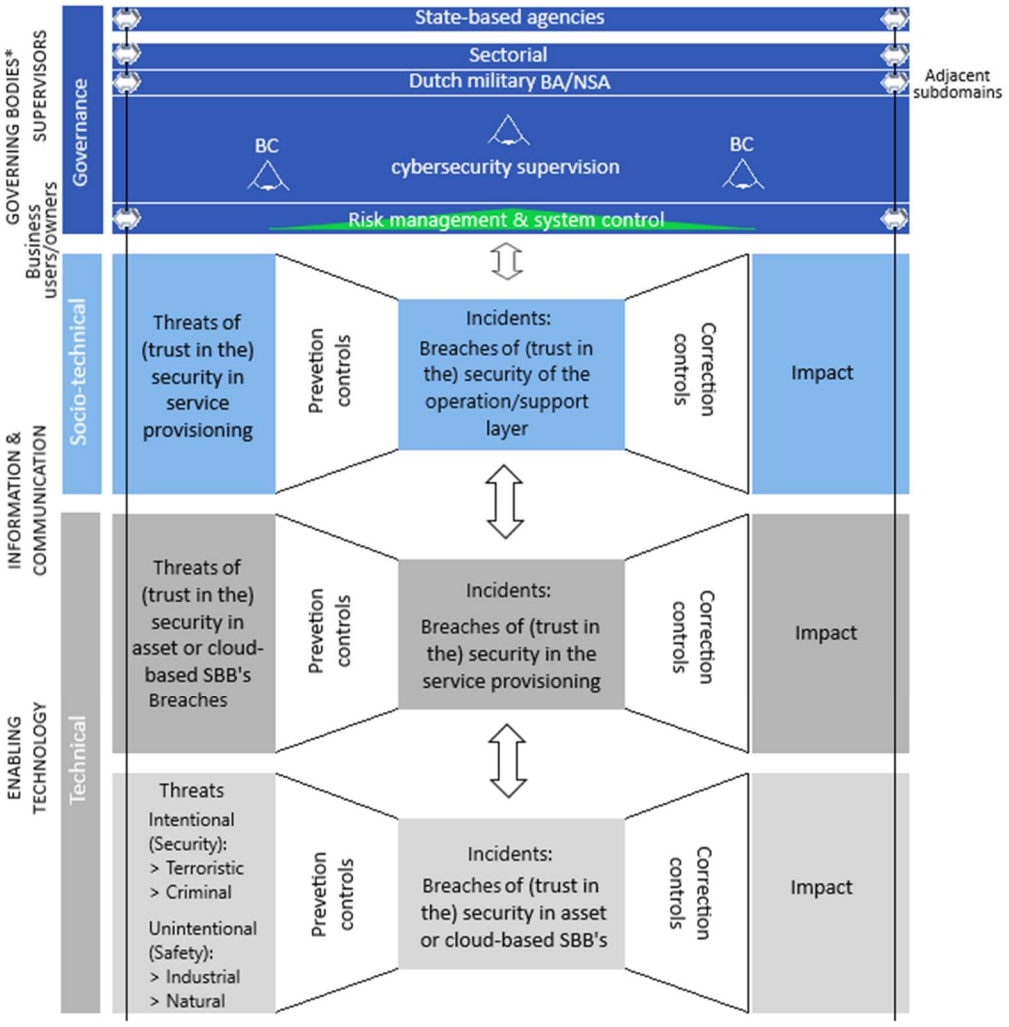
The threat event in Table 5 results in a Medium risk level (5). According to Table 6, the supervisor decides that the regulatee must follow the risk modification strategy. The regulatee must implement controls (countermeasures) to reduce the risks to acceptable risks (green area) for the owner within a fixed time frame. Based on the risk assessment result in Table 5, the countermeasure (control) is, for example, improved training in cybersecurity skills. Ideally, users are unknowingly cybersecurity-skilled. That is, unconscious behavior is characterized by automatic actions based on habits. An automatic operation is ideal when a few mistakes are allowed in a stable environment; however, ensuring diverse work is also essential when the environment changes quickly. [89] Another way of training end users in case of mistakes is creating a corporate cybersecurity culture in the military domain. [90]

(f) Design and implement cyber controls (countermeasures) for handling risks

The “Bowtie” model visually represents the relationship between threats, prevention controls, (inter)dependent incidents, repression controls, and impact (risks)/consequences for the Dutch military operations/support activities. See Figure 8, subsection 2.2.2.
From the supervisor's perspective, the critical event in the operation/support layer is a breach of trust in the agreed (among stakeholders/owners) security of the provided IT platform application services. The critical event in the provider layer is a breach of trust in the security of the IT platform service provisioning equipment, such as asset-based antennas, radio/telecom equipment, cables, and satellites. Likewise, the critical event in the service layer is a breach of trust in the security of the IT platform services such as crypto services, IaaS, PaaS, and Saas cloud services. See also subsection 2.3.3 or Figure 29 (APPENDIX J).

As a result of cascading effects into adjacent subdomains supporting Dutch military and partner units, a breach of trust in the security of the IT platform service layer threatens the provider layer. At the same time, a breach of trust in the security of the provisioning layer threatens the operation/ support layer (bottom-up).
Note: A cascade effect can also go top-down. For example, risks can be too high when an IT platform owner lacks proper training in cybersecurity skills. An IT platform service owner's *trade-off* may result in inadequate agreed service levels. The provider may then implement insufficient security measures,

such as weak encryption, to compensate for performance issues, but the risks are too high, according to security regulations. The cybersecurity supervision model layers depicted in Figure 14 are combined with Figure 8 and presented in Figure 15. The (visualisation of the) cacsading effect using the "Bowtie" for the socio-technical and technical layers is inspired by the master thesis "Can NL trust 5G?" by Farley Wazir. [9] The improved IT platform model visually presents for each model layer the threats, prevention and correction controls, (inter) dependent incidents (the cascading effects), and the impact (risks) / consequences on the Dutch military, sectors, and society.



*BOD: composed of (non) executive directors

FIGURE 15 'BOW TIE' & THE CYBERSECURITY SUPERVISION MODEL WITH CRITICAL EVENTS & CASCADING EFFECTS

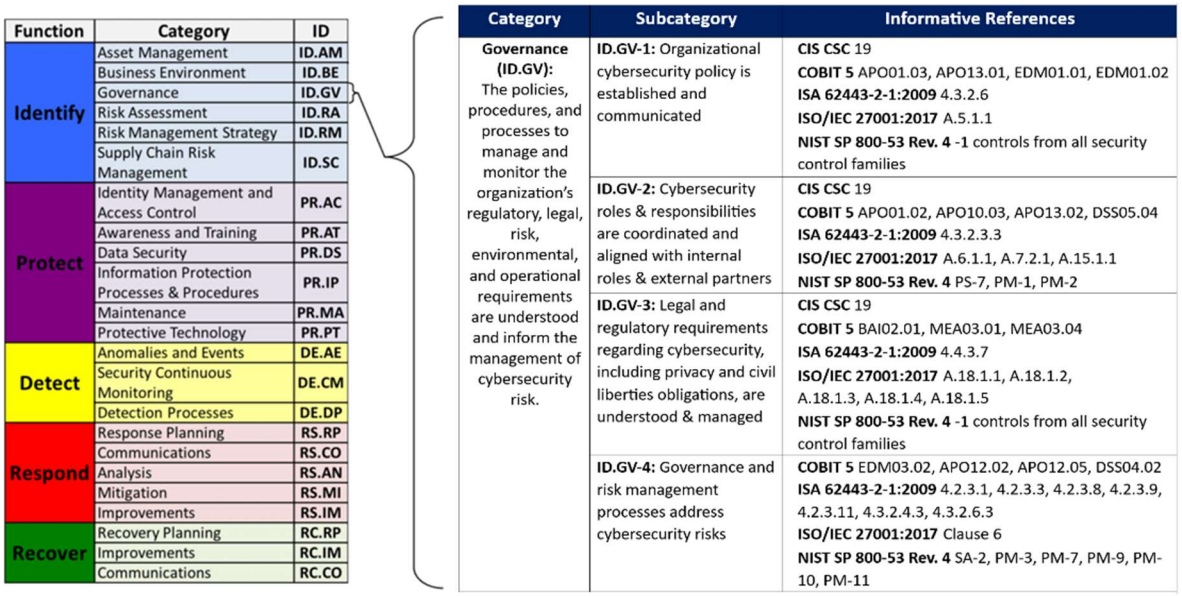
Proposal of prevention and correction controls

Regulatees account to the supervisor for security by design, security by default, [91] with the owner responsible for implementing prevention and correction controls "to ensure a level of security appropriate to the risk" [63]; this obligation is part of the accountability and compliance principle based on the EU GDPR (and NIS/NIS2) transposed to Dutch law and supplemental Dutch military self-regulations. See subsections 3.3.2 and 3.3.3. The prevention controls aim to (a) identify risks and prevent incidents given the threats and their impact. It is also about (b) protecting the assets. The aim is to implement countermeasures to protect the assets identified as critical. Before implementing preventive measures, it is important to realize that there is no 100% security. Preventive controls are essential but are not always efficient from a functional and cost perspective.

Therefore, there is increasing attention to repressive controls to identify threats and respond promptly and adequately. Because, with the *digital transformation*, it is no longer a question of whether an incident will occur but when. Correction controls concern (c) detecting unwanted use of IT platform assets, (d) responding to undesirable behavior, and (e) recovering from damage. [33]

Supervision/owner (governance) layers

When we map the above controls (a-e) to the supervision/owner (governance) layers of Figure 15, preventive measures include creating cyber security awareness. Other security objectives and controls for the supervision/owner (governance) layers are described in sections 2.1 and 2.2. Section 2.3 explains the Dutch military context for meeting the security objectives. The objectives for the cybersecurity supervision/owner (governance) controls include developing a cybersecurity policy framework, implementing cybersecurity roles and responsibilities, and implementing governance and risk management systems that address cybersecurity risks. These objectives align with objectives for the Governance controls part of the cybersecurity NIST framework [81] shown right of Figure 16.



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Category	Subcategory	Informative References
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2017** A.5.1.1 **NIST SP 800-53 Rev. 4** -1 controls from all security control families
	ID.GV-2: Cybersecurity roles & responsibilities are coordinated and aligned with internal roles & external partners	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2017** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood & managed	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2017** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 4** -1 controls from all security control families
	ID.GV-4: Governance and risk management processes address cybersecurity risks	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2017** Clause 6 **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11

FIGURE 16 CATEGORIES OF CONTROLS WITH REFERENCE TO INDUSTRY CYBERSECURITY CONTROL FRAMEWORKS [81]

The objectives of the prevention and corrections controls (a) - (e) are presented in the "Function" column on the left. The functions are a set of activities to achieve specific cybersecurity outcomes. The "*Categories*" column represents subdivisions of functions into groups of cybersecurity outcomes closely tied to organizational (programmatic) needs and particular activities in managing and supervising cybersecurity risks. For example, the governance "*Subcategory*" activities highlighted on the right side of Figure 16 relate to the preventive "*Identify"* function. The "Informative References" column lists specific standards, guidelines, and practice sections.
Tailored to its context, an organization can add a cyber security supervision *subcategory* to the governance control *category*. Controls may focus on the identified requirements for the cybersecurity supervision model. For example, controls that focus on the effectiveness of risk management and control systems (design requirement 4). These controls are part of the supervision layer visualized in Figure 16 to ensure the trustworthiness of the IT platform services.
Trustworthiness to its users, stakeholders, and society, with the mandated owner and BOD ultimately responsible. The cascading effects concern the threats arising from breaches of trust in the security of the cybersecurity supervision model layers. The owner must convince the supervisory body about adequate cybersecurity based on evidence to earn trust.

Support & operation (socio-technical) layers

When we map the controls to critical cyber activities in the support and operation layers, preventive controls aim to improve cybersecurity user (producers and consumers) awareness to achieve adequate behavior and to enhance cyber competencies, among others, by executing crisis exercises. Repressive controls include reporting to the line management and supervisor about unusual user behavior. [33] Other examples are controls that reward good user behavior or corrective measures for bad user behavior. The corrective measure can be a fine or the obligation to eliminate temporarily accepted risks with a convincing (for the supervisor) improvement plan within an agreed time frame.

Provider & service (technical) layers

Preventive controls for the provider layer (communication/network) assets consist of measures (with the objective) to protect the availability, integrity, and confidentiality of critical information. The preventive controls for securing the service layer (cloud-based) assets have the same objective. The objectives are achieved with the implementation of physical measures (for example, secure access to a physical location with IT systems), logical measures (software/cloud-based), personnel measures (screening), security by design (for example, compartmentalization, defense in depth and crypto), secure development and testing of hardware and software, certification, secure interfaces, and patch management. Repressive controls concern the obligation (legal obligation for vital processes) to disclose a breach by the IT service provider. Other examples are controls such as network monitoring, malware protection, or data recovery.

(g) Monitoring and review

The non-executive BOD directors should supervise the policies carried out by the executive directors and, in doing so, should focus on the effectiveness of the organization's risk management and control systems. [2] Risk management is an ongoing process, and changes in any facet will necessitate updating & re-evaluating by the mandated IT platform owner of the previously decided acceptable risk levels and selected security controls.

The iterative steps are triggered again in the event of non-compliance for appropriate operational, structure/tactical, or strategic adjustments.

SA and Sensemaking support the mandated supervisor(s) in monitoring the effectiveness of the implemented controls. Again, a critical boundary condition is cooperation between the supervisors of adjacent subdomains. [37] [38]

Following the Bowtie, when controls fail or do not work as intended, for example, due to contradictions or different interpretations of controls, the need for proposing additional "*escalation factor*[92]*"* controls arises for a robust and effective management system (design requirement 4). [35]

4.2 Building the cybersecurity supervision model

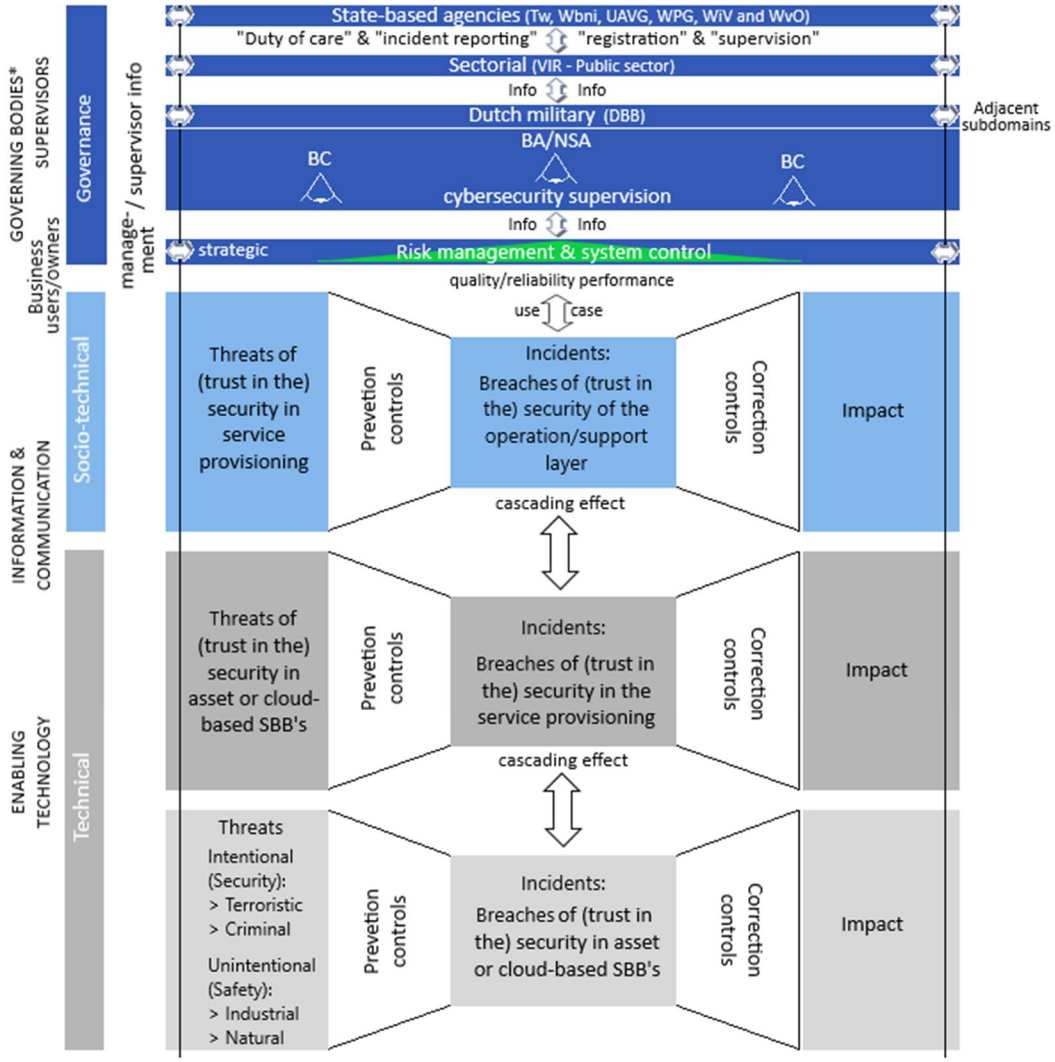
The objective (see section 1.2) is *"to design an integrated cybersecurity supervision model for the Dutch military domain."* Supervisors aim to ensure stakeholder trust in IT platform services by demonstrating end-to-end security for adjacent series of subdomains in cyberspace (Figure 1).

The first requirement, explained in the previous section, demands a (1) risk-based approach to cybersecurity supervision, considering cascading effects.

The remaining design requirements specified in section 3.5 imply high interactions within the cyber security supervision layer: (2) cooperating supervisory bodies, (3) harmonizing their norms, (4) information gathering and compliance monitoring, and (5) intervention (if needed).

[92] Escalation factors: "conditions that lead to increased risk by defeating or reducing the effectiveness of barriers," also called Defeating Factors or Barrier Decay Mechanisms. In other words, Escalation Factors create the holes in the Swiss Cheese Model of James Reason. [116]

Figure **17** presents the final integrated cybersecurity supervision model for the Dutch military domain.



*Dutch military one-tier BOD: composed of senior (non) executive directors

FIGURE 17 THE INTEGRATED CYBERSECURITY SUPERVISION MODEL FOR THE DUTCH MILITARY DOMAIN

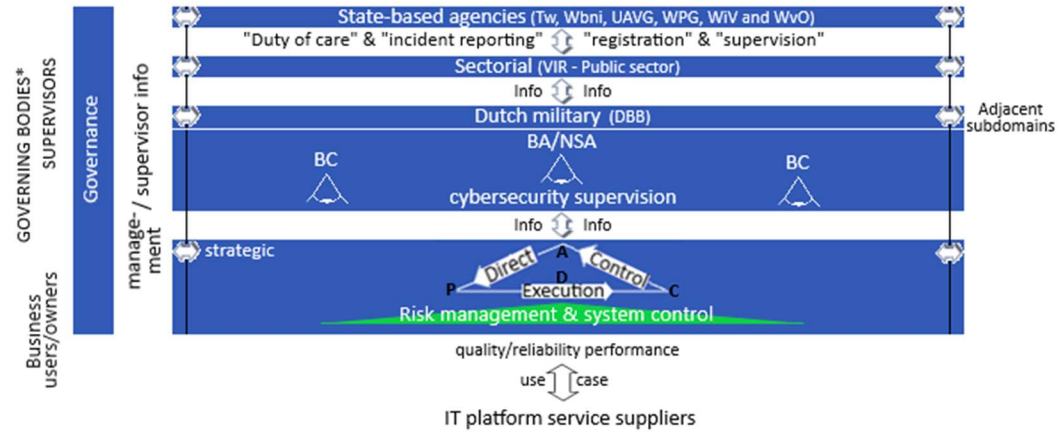
The final integrated cybersecurity supervision model meets all the remaining design requirements:

2. Cooperation between supervisors of adjacent subdomains that support Dutch military and partner units;
3. Application of mutually accepted and up-to-date cybersecurity control frameworks;
4. Collect information from supervisors from the growing number of Dutch military and partner units to create situational awareness. Units with, for example, IT service contractors and sub-contractors. Supervisors address this by focusing on the effective operation of a risk management and control system and their mutual coordination in monitoring compliance. Therefore, supervisors must focus on systemic risks (and some "*random security tests*[93]") instead of time-consuming low-level risks (treatment of symptoms);

[93] Random security tests: desk research (setup), acceptance tests (existence), or penetration tests (exploitation).

5. Intervene in the event of non-compliance, considering systemic risks (with cascading effects) and using up-to-date controls accepted by supervisors for adjacent subdomains supporting the diverse Dutch military and partner units.

Figure 18 illustrates the information flow between the supervisors (BC/BA/NSA and state-based agencies), the owner(s), and the IT platform service supplier(s).



* Dutch military one-tier BOD: composed of senior (non) executive directors
** BOD / Mandated supervisors and owners of partner units enabled by the adjacent subdomains

FIGURE 18 INFORMATION FLOW BETWEEN SUPERVISOR, OWNER, USER, AND IT PLATFORM SERVICE SUPPLIER ROLES

Table **7** explains the cybersecurity information exchange between the suppliers (of services), owners (also representing users), cooperating supervisory bodies, and BOD following the PDCA and Direct Control cycle steps. Ultimately, the IT platform service owner must convince its assigned supervisor based on evidence of implemented cybersecurity controls. After providing accountability for compliance with cybersecurity regulations via an "Approval Request" (step VII), IT platform service owners receive an "Approval to Operate" from the supervisor within their regulatory area (step VIII).

	Plan	**Do**	**Check**	**Act***
Suppliers (and services)	**I(a)** Execute impact analysis	**II** Design/build **V** Execute risk classification	Verify → **VI'**: **III** Implemented controls check **IV** Quality check	**VI'** Continuously implement improvements
Mandated **owners** (also representing users)	**I(b)** Determine reliability **I(c)** Proposal to BC/BA for composition of approval documen-tation.	**VI** Determine risk handling: **(a)** (temporal) risk acceptance/rejection **(b)** Sign Statement of Compliance (SOC/SOC-Interface) **(c)** Improvement Plan **VII** Approval Request		
Mandated **supervisors** (and exchange with state-based agents and supervisor bodies of adjacent subdomains)	**I(d)** Determine approval documen-tation.		**VIII** Issuing Approval /Rejection: **(a**) (Interim) Approval to Operate **(b)** Certification of interface **(c)** System-oriented and some "*random security tests*";	**VIII(b)** Issuing (temporal) approval or rejection → **VI'**
BOD			**Control** in the event of escalation to the BOD.	**Direct** in the event of strategic adjustments.

* Report to state base agent(s) according to government regulations (“Duty of care,” “Incident reporting,” “Registration” and “Supervision”)

TABLE 7 INFORMATION EXCHANGE REGARDING CYBERSECURITY BETWEEN THE SUPPLIERS (OF SERVICES), OWNER (AND USERS), SUPERVISORY BODIES, AND BOD FOLLOWING THE PDCA AND DIRECT CONTROL CYCLE STEPS OF FIGURE 18

APPENDIX P (Figure 31) explains the cybersecurity information exchange in more detail based on the VIII steps in Table **7**.

4.3 Design evaluation of the cybersecurity supervision model

This section evaluates the Dutch military cybersecurity supervision model, following step E1 (section 1.3) and Hevner guideline 3 (APPENDIX A). The evaluation is based on information collected to grant (interim) approval for operating fourteen Dutch military-critical IT platform services. [10] The owners must convince the BA of implemented cybersecurity controls (steps VII and VIII of Table 7). In practice, collecting evidence proves to be a challenge. When owners request an IT platform service Approval To Operate (ATO), the evidence is not always convincing. The supervisors of partners of the Dutch military often see similar challenges.

For example, regarding the Dutch military critical Border Patrol IT platform services, the partner is the Ministry of Justice and Security and (sub) contractors in the private sector (PPP). The critical IT platform services supporting Schiphol border control processes are considered vital for Dutch society by the Wbni. [58] See subsection 3.3.2 and the Court of Audit report “Digitization at the border.” [92]

Establishing governance agreements between the Dutch military units mutually and units of the Ministry of Justice and Security and (sub) contractors in the private sector (PPP) is complex. The agreements require clear responsibilities in handling risks for users (cyber activities/processes versus process domain owners), ownership of the enabling IT platform services, and processed information. Otherwise, managing and supervising critical cybersecurity controls to mitigate high risks (including prioritization within the boundary conditions) will be challenging.

Operating an organization-wide compliance and risk management system also remains challenging, especially with cybersecurity being one of the aspects to be managed and supervised in cooperation with its partners (see 2.4-3) in the public and private sectors.
In the event of non-compliance, adjustments by the mandated owner(s) require cybersecurity SA and Sensemaking (see section 2.2.2) to manage risks with cascading effects.
Hereafter, when sufficient insight is lacking by the owners, managing risks and adjusting based on improvement plans is challenging. Consequently, in practice, the owner repeatedly requests the supervisor to extend the previously issued Interim Approval To Operate (IATO) and, thus, a more extended period of acceptance of high risks.

In practice, organization-wide implementation of a compliance and risk management system (with cybersecurity as one of the aspects) within the Dutch military and partners appears insufficient. Therefore, supervision of its effective operation regarding cybersecurity remains essential. As a result, implementing the integrated cybersecurity supervision model for the Dutch military domain is not entirely possible. In that case, the focus remains on time-consuming checks of many cybersecurity controls (symptoms treatment) rather than systematic risks.

However, the evaluation also shows that the model can be used to grow into an effective compliance and risk management system (and improve cybersecurity situational awareness and sensemaking). The result will ultimately be a fully integrated cybersecurity supervision model for the Dutch military domain.

6. Conclusions & recommendations

An integrated cybersecurity supervision model has been designed for the Dutch military domain through several intermediate steps based on the identified design requirements.
The model depicted in Figure **19** comprises an integrated risk-based supervision approach involving the owner, operations/support, provider, and service subdomain layers and coordinating between the Dutch military and partner units for information collection and compliance monitoring.

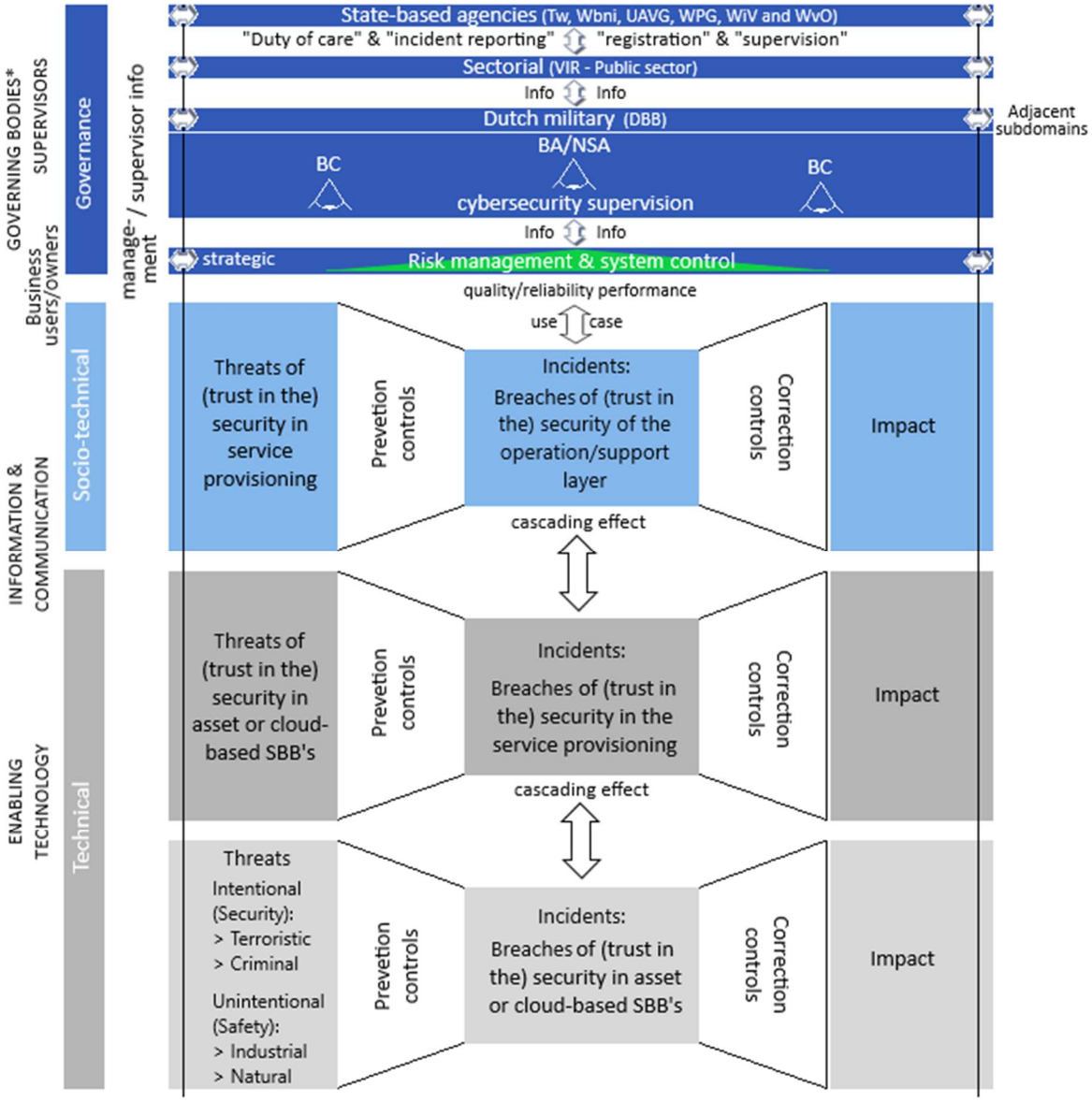


FIGURE 19 THE INTEGRATED CYBERSECURITY SUPERVISION MODEL FOR THE DUTCH MILITARY DOMAIN

The model demonstrates critical events resulting in risks with cascading effects in each adjacent subdomain layer. The information collection contains relevant control frameworks, threats, risk assessments, systematic risks with cascading effects, and interventions substantiated with retrievable IT management and design documents for creating security awareness. Stakeholder trust in the end-to-end security of IT platform services is increased and maintained by the model.

Following the Hevner design science guidelines, the Dutch military cybersecurity supervision model is evaluated based on (interim) approvals for operating fourteen Dutch military-critical IT platform services issued by the BA. [10]

In practice, organization-wide implementation of a compliance and risk management system as part of the owner/management layer (with cybersecurity as one of the aspects) appears insufficient. As a result, implementing the integrated cybersecurity supervision model for the Dutch military domain is not entirely possible. In that case, the focus remains on time-consuming checks by the supervisor of many cybersecurity controls (symptoms treatment) rather than systematic risks.
However, the evaluation also shows that the model can be used to grow into an effective compliance and risk management system (and improve cybersecurity situational awareness and sensemaking). The result will ultimately be a fully integrated cybersecurity supervision model for the Dutch military domain.

5.1 Recommended steps for implementation

To implement the integrated cybersecurity supervision model, the Dutch military supervisory body (BA) should initiate the following recommended steps:

1. Identify all supervisors and IT platform service owners of Dutch military and partner units of adjacent subdomains;
2. Establish governance agreements between the Dutch military units mutually and units of public/private sector partners. The agreements must contain clear responsibilities in process domain owners handling user risks (cyber activities/processes), ownership of the enabling IT platform services, and processed information. The goal is to identify responsible owners and supervisors for managing and supervising cybersecurity controls;
3. Implement an effective risk and compliance management system considering systematic risks with cascading effects into adjacent subdomains;
4. Request agreements between supervisors and IT platform service owners (with the IT platform users and IT platform service suppliers reporting on security performance) of adjacent subdomains on:
    a. mutually accepted and up-to-date cybersecurity control frameworks;
    b. collecting information for supervising compliance with cybersecurity regulations for IT platform services;
5. Implement an information exchange between the relevant state-based agents and organizational supervisors regarding information exchange on cybersecurity legislation;
6. Emphasize the independent role of the supervisor to maintain (multi)stakeholder trust in the provisioning of secure IT platform services;

5.2 Communication

The integrated cybersecurity supervision model is presented to the BA staff.
They were pleased with the model's insight into the risks with cascade effects into adjacent subdomains, ensuring the cyber security of IT platform services and the need for cooperation between supervisory bodies. The eight-step plan is adopted and converted into formal BA instruction.

5.3 Future work recommendations

Analyze the applicability of the Dutch military integrated cyber security supervision model with partners of the Dutch military. Based on the outcomes, the model might be refined.Compare the Dutch military integrated cyber security supervision model with the supervision models of relevant partners.
Considering the limitations imposed by the regulatory environment, explore what further regulations are required to make it more straightforward for the involved stakeholders to ensure the cyber security of IT platform services.

References

[1] H. Nissenbaum, “Securing Trust Online: Wisdom or Oxymoron,” *Bost. Univ. Law Rev.*, pp. 101–131, 2001, doi: 10.1525/sp.2007.54.1.23.

[2] Monitoring Committee, “The Dutch Corporate governance code,” no. December. 2022.

[3] J. Van Den Berg *et al.*, “On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education,” *NATO STO/IST-122 Symp. Tallin*, no. c, pp. 1–10, 2014.

[4] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, “Kaderstellende visie op toezicht,” no. 1. Sdu Uitgevers, p. 27, 2001.

[5] WRR, “Toezien op publieke belangen.” Amsterdam University Press, Amsterdam, p. 183, 2013.

[6] Tweede Kamer der Staten-Generaal, “Minder last , meer effect.” Tweede Kamer der Staten-Generaal, Den Haag, p. 39, 2005.

[7] M. Lodge and K. Wegrich, “Managing Regulation: Regulatory Analysis, Politics and Policy.” Palgrave Macmillan, p. 276, 2012.

[8] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design Science Research in Information Systems,” *Syst. Q. J. Assoc. Inf. Syst.*, vol. 28, no. 85, pp. 75–105, 2004, doi: 10.2307/25148625.

[9] F. Wazir, “Can NL trust 5G?,” Leiden University, 2019. [Online]. Available: https://studenttheses.universiteitleiden.nl/handle/1887/87821?solr_nav%5Bid%5D=59925288b1ceb42138cc&solr_nav%5Bpage%5D=1&solr_nav%5Boffset%5D=12

[10] Ministerie van Defensie, “Toezichtjaarverslag 2022 Beveiligingsautoriteit,” 2023, [Online]. Available: https://www.rijksoverheid.nl/documenten/jaarverslagen/2023/05/17/jaarverslag-beveiligingsautoriteit-over-2022

[11] R. Schenk and P. Smallegange, “IT-innovatie bij Defensie : een bimodale aanpak,” no. 20, 2018.

[12] Ministerie van Defensie, “Defensienota 2018.” 2018.

[13] Ministerie van Defensie, “Nederlandse Defensie Doctrine voor Militaire Cyberspace Operaties.” MOD, p. 58, 2018.

[14] S. Köffer, K. C. Ortbach, and B. Niehaves, “Exploring the relationship between IT consumerization and job performance: A theoretical framework for future research,” *Commun. Assoc. Inf. Syst.*, vol. 35, pp. 261–283, 2014, doi: 10.17705/1cais.03514.

[15] T. Breene and P. Nunes, “Reinvent Your Business Before It ’ s Too Late,” *Harv. Bus. Rev.*, no. February, pp. 80–88, 2011, [Online]. Available: hbr.org.%5CnHBR Reprint R1101D

[16] Ministerie van Defensie, “Direction SG-002 ‘Governance at Defense.’” Ministry of Defence (NL), The Hague, p. 78, 2021.

[17] B. Y. B. Edelman and D. Geradin, “Pipelines, Platforms and the New Rules of Strategy,” *Harv.*

Bus. Rev., no. April, pp. 2012–2014, 2016.

[18] Ministerie van Defensie, “IT-strategie 2019-2024.” MOD, pp. 1–32, 2018.

[19] R. Maes, D. Rijsenbrij, O. Truijens, and H. Goedvolk, “Redefining business: IT alignment through a unified framework,” *Primav. Work. Pap.*, vol. 19, p. 25, 2000.

[20] Government of the Netherlands, “Besluit BVA-stelsel Rijksdienst 2021.” Staatscourant, pp. 1–11, 2020.

[21] Ministerie van Defensie, “Defensie cyber strategie.” pp. 1–18, 2018.

[22] Ministerie van Defensie, “Defensie High-Level IT-ontwerp,” 2015. https://zoek.officielebekendmakingen.nl/blg-523384 (accessed Jan. 04, 2023).

[23] Ministerie van Defensie, “Derde BIT-advies programma ‘Grensverleggende IT’ Bestuursstaf.” 2019.

[24] A. (Andres) Bulk, “Federated Mission Networking,” *Intercom (Des. Moines).*, vol. 1, no. 46, pp. 27–34, 2017.

[25] NCTV and NCSC, “Cybersecuritybeeld nederland 2023,” *Csbn*, pp. 1–76, 2023, [Online]. Available: https://www.thehaguesecuritydelta.com/media/com_hsd/report/237/document/CSBN2019-online-tcm31-392768.pdf

[26] R. Wieringa, “Design Science as Nested Problem Solving,” *Int. Conf. Des. Sci. Res. Inf. Syst. Technol.*, pp. 1–12, 2009.

[27] Gartner, “Bimodal IT : How to Be Digitally Agile Without Making a Mess,” *Each Exec. Programs*, no. 5, pp. 1–58, 2014.

[28] 123management, “What is the Nine-Head Model ? Relationship nine-plane model and the control frame Information management processes : ICT management,” *123management*, 2017. http://123management.nl/0/020_structuur/a232_structuur_03_informatie_management_9vlaks.html (accessed Jan. 13, 2023).

[29] R. von Solms and S. H. (Basie) von Solms, “Information Security Governance: A model based on the Direct-Control Cycle,” *Comput. Secur.*, vol. 25, no. 6, pp. 408–412, 2006, doi: 10.1016/j.cose.2006.07.005.

[30] R. Von Solms and J. Van Niekerk, “From information security to cyber security,” *Comput. Secur.*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[31] L. Kiely and T. Benzel, “Systemic Security Management: A new conceptual framework for understanding the issues, inviting dialogue and debate, and identifying future research needs,” p. 3, 2006.

[32] IT Governance Institute, “An Introduction to the Business Model for Information Security,” p. 28, 2009.

[33] B. Hulsebosch and A. van Velzen, “Inventarisatie en classificatie van standaarden voor cybersecurity Colofon,” The Hague, 2015.

[34] ISO, “ISO 31000:2018(en) Risk management — Guidelines,” *Online Browsing Platform (OBP)*,

2018. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en (accessed Mar. 26, 2023).

[35] Wikipedia-Community, “Bow-tie diagram.” https://en.wikipedia.org/wiki/Bow-tie_diagram (accessed Aug. 27, 2023).

[36] W. Tewarie, “SIVA-methode voor de ontwikkeling van auditreferentiekaders.” UWV/CIP, 2015.

[37] M. R. Endsley, “Towards a Theory of Situation Awareness in Dynamic Systems,” *Hum. Factors*, vol. 37, no. 1, pp. 32–64, 1995.

[38] Wikipedia-Community, “Situation awareness,” *Wikipedia.org*. https://en.wikipedia.org/wiki/Situation_awareness (accessed Jul. 10, 2023).

[39] Ministerie van Defensie, “Defence Vision 2035.” Ministry of Defence (NLD), The Hague, p. 64, 2020. [Online]. Available: https://english.defensie.nl/downloads/publications/2020/10/15/defence-vision-2035

[40] H. Fayol, “General and Industrial Mangaement.” p. 110, 1949. [Online]. Available: https://ia801600.us.archive.org/4/items/in.ernet.dli.2015.13518/2015.13518.General-And-Industrial-Management.pdf

[41] J. E. Andriessen and F. Hartog, “De sociaal-economische besturing van Nederland,” 1970.

[42] K. Bleicher, *Das Konzept integriertes management*. Campus Verlag Frankfurt, 1991.

[43] R. I. Tricker, *Corporate governance: Practices, procedures, and powers in British companies and their boards of directors*. Gower Publishing Company, Limited, 1984.

[44] Ministerie van Defensie, “Eindrapport DoIT Rompdocument.” Tendernet, 2015. [Online]. Available: https://www.tenderned.nl/tenderned-tap/aankondigingen/62227;section=2

[45] M. Vertegaal, “Development of a Battlefield Management System : how to use the user,” no. January. pp. 1–14, 2002. [Online]. Available: http://www.dodccrp.org/events/6th_ICCRTS/Tracks/Papers/Track2/003_tr2.pdf

[46] G. B. Skip and D. Jr, “The future of NATO C4ISR.” Atlantic Council, 2023. [Online]. Available: https://www.atlanticcouncil.org/wp-content/uploads/2023/03/The-future-of-NATO-C4ISR-Assessment-and-recommendations-after-Madrid.pdf

[47] D. Janezic, “FMN for Coalition Operations,” *AFCEA – Bonn, DEU– 22-23 June 2016*, 2016. https://www.afcea.de/fileadmin/user_upload/Sonderveranstaltungen/FA_mit_FueUstgKdoBw/13-NCIA-FMN1.pdf (accessed Aug. 29, 2020).

[48] Leidos, “C4ISR - The Military’s Nervous System,” *Defense One*, 2020. https://www.defenseone.com/insights/cards/c4isr-military-nervous-system/ (accessed Aug. 30, 2020).

[49] S. Farahmandian and D. B Hoang, “Security for Software-Defined (Cloud, SDN and NFV) Infrastructures - Issues and Challenges,” pp. 13–24, 2016, doi: 10.5121/csit.2016.61502.

[50] T. J. Betcher, S. Disaster, and R. Coordinator, “Cloud Computing: Key IT-Related Risks and Mitigation Strategies for Consideration by IT Security Practitioners,” vol. 1277, no. February 2010, 2010.

[51] NATO, “NATO Interoperability Standards and Profiles NATO STANDARD ADatP-34(L) / Version

12," vol. 1, no. L. Allied Data Publication, 2019.

[52] K. S. Cameron and R. E. Quinn, *Diagnosing and changing organizational culture. Revised edition.*, vol. 16, no. 1. 2006.

[53] Inspectieraad, "Programma Innovatie Toezicht." Buireau Inspectieraad, Den Haag, 2018.

[54] L. Lessig, "C o d e 2.0." Basic Books, New York, p. 402, 1999.

[55] EAR, "Enterprice Architecture Civil Service (EAR)." https://www.earonline.nl/ (accessed Jun. 25, 2022).

[56] NORA, "NORA." https://www.noraonline.nl/wiki/Kaders_beveiliging (accessed Jun. 25, 2022).

[57] Dutch Ministry of Economic Affairs Agriculture and Innovation, "Telecommunications Act." The Hague, pp. 1–88, 2012.

[58] Dutch Department of Justice and Security, "Wet beveiliging netwerk- en informatiesystemen," *Staatsblad*, pp. 1–11, 2018.

[59] European Union, "NIS Directive," *European Union*. pp. 1–30, 2016. doi: 10.2307/j.ctt1xhr7hq.20.

[60] Rijksoverheid, "Wet op de inlichtingen- en veiligheidsdiensten 2017." Rijksoverheid, pp. 8–10, 2017.

[61] The European Parliament and the Council of the European Union, "DIRECTIVE (EU) 2018/1972 establishing the European Electronic Communications Code (Recast)," no. July 2002. pp. 36–214, 2018. [Online]. Available: https://ec.europa.eu/digital-single-market/en/desi

[62] European Commission, "Evaluation of the ePrivacy Directive 2002/58/EC," 2017, [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0005&from=EN

[63] European Parliament and the Council of the European Union, "General Data Protection Regulation (GDPR)." 2016.

[64] European Parliament and the Council of the European Union, "NIS 2 Directive," *Off. J. Eur. Union*, vol. 2022, no. November, pp. 80–152, 2022, [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[65] European Union, "Types of EU legislation," *European Union*, 2020. https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en (accessed Sep. 08, 2023).

[66] Government of the Netherlands, "Uitvoeringswet Algemene verordening gegevensbescherming (AVG)." Staatscourant, pp. 1–13, 2016. [Online]. Available: https://wetten.overheid.nl/BWBR0040940/2019-02-19#Hoofdstuk3

[67] Government of the Netherlands, "Wet politiegegevens (WPG)." Staatscourant, The Hague, pp. 1–23, 2007.

[68] Prof. dr. Heinrich Winter, Dr.ir. Bieuwe Geertsema, Mr. Thijs Drouen, Mr. Ernst van Bergen, and Mr. Christian Boxum, "Naleving van de AVG door overheden," no. december, 2022, [Online]. Available: www.pro-facto.nl

[69] Rijksoverheid, "Baseline Informatiebeveiliging Overheid (BIO) versie 1." Rijksoverheid, Den

Haag, 2020.

[70] Rijksoverheid, “Wet veiligheidsonderzoeken,” 2015, [Online]. Available: https://wetten.overheid.nl/BWBR0008277/2015-09-01

[71] European Commision, “EU Electronic Communications Code.” https://digital-strategy.ec.europa.eu/en/policies/eu-electronic-communications-code#:~:text=The Code protects consumers irrespective,online banking%2C and video calls (accessed Aug. 07, 2023).

[72] S. E. Donaldson, S. G. Siegel, C. K. Williams, and A. Aslam, “Cybersecurity Frameworks BT - Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats,” S. E. Donaldson, S. G. Siegel, C. K. Williams, and A. Aslam, Eds. Berkeley, CA: Apress, 2015, pp. 297–309. doi: 10.1007/978-1-4302-6083-7_17.

[73] K. I. Alshitri and A. N. Abanumy, “Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia,” in *2014 International Conference on Information Science & Applications (ICISA)*, 2014, pp. 1–4. doi: 10.1109/ICISA.2014.6847396.

[74] R. Ali, “Technological Neutrality,” 2009. http://www.aber.ac.uk/media/Documents/tecdet/tecdet.html. (accessed Jul. 23, 2023).

[75] NATO, “AC/35-D/2005-REV3 MANAGEMENT DIRECTIVE ON CIS SECURITY,” vol. 3, no. October. 2015.

[76] ISO/IEC, “Nen-iso/iec 27001,” vol. 27001, no. november 2005, 2005.

[77] NEN, “NEN-EN-ISO/IEC 27002 (nl).” Koninklijk Nederlands Normalisatie-instituut, Delft, 2017.

[78] MIVD, “ABDO (Algemene Beveiligingseisen Defensie Opdrachten).” 2018.

[79] NATO, “AC/322-D/0048-REV3 (INV) - Technical and implementation directive for CIS Security.” NATO, p. 97, 2019.

[80] Ministerie van Defensie, “Aanwijzing SG 948 Toezicht bij Defensie.” MOD, The Hague, p. 3, 2016.

[81] M. Barrett, “Framework for improving critical infrastructure cybersecurity,” *Proc. Annu. ISA Anal. Div. Symp.*, vol. 535, pp. 9–25, 2018.

[82] ISO/IEC, “Nen-iso/iec 31010,” 2014.

[83] Ministerie van Defensie, “Vuistregels gebruik e-mail- en internetvoorzieningen Defensie,” 2024. file:///C:/Users/hp/Downloads/Vuistregels gebruik e-mail- en internetvoorzieningen Defensie.pdf

[84] Defensie sociale veiligheid & integriteit, “Gedragsregels Defensie Sociale Veiligheid,” pp. 1–5, 2020, [Online]. Available: https://puc.overheid.nl/mp-bundels/doc/PUC_100060001010_10/1/

[85] NIST, “Guide for Conducting Risk Assessments,” *Special Publication (NIST SP) - 800-30 Rev 1*, no. September. NIST, p. 95, 2012. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-30r1

[86] NIST, “Risk Management Guide for Information Technology Systems,” *NIST Special Publication 800-30*, vol. 29, no. 1. pp. 44–45, 2002.

[87] Enisa, “Cramm Product identity card,” *ENISA*, 2023. https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html (accessed Oct. 23, 2023).

[88] NEN, “NEN-ISO/IEC 27005.” Koninklijk Nederlands Normalisatie-instituut, Delft, p. 64, 2018.

[89] P. Overbeek, E. R. Lindgreen, and M. Spruit, *Informatiebeveiliging onder controle*. Pearson Benelux B.V., 2005. [Online]. Available: https://books.google.nl/books?hl=nl&lr=lang_nl&id=03A4363JQd4C&oi=fnd&pg=PA7&dq=online+marketing&ots=ODnpzynscc&sig=-ImcjM4fZTYvTV7egVnPpdXYXB4

[90] J. Duynhouwer, “7 aspecten van security by design en security by default,” *Computable*, 2018. https://www.computable.nl/artikel/blogs/security/6305605/5260614/7-aspecten-van-security-by-design-en-security-by-default.html (accessed Oct. 24, 2023).

[91] J. Duynhouwer, “7 aspecten van security by design en security by default,” *Computable*, 2018.

[92] Netherlands Court of Audit, “Digitalisering aan de grens.” Den Haag, p. 53, 2020.

[93] ISO/IEC, “ISO/IEC 38500.” 2008.

[94] ISACA., *COBIT 5: A business framework for the governance and management of enterprise IT*. Isaca, 2012.

[95] Ministerie van Defensie, “Visie op IT: let’s make IT happen!,” pp. 1–12, 2014.

[96] European Commission, “Proposal for an ePrivacy Regulation,” 2017. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation (accessed Aug. 07, 2023).

[97] European Union Agency for Fundamental Rights and The Council of Europe, “EU charter of fundemental rights.” https://fra.europa.eu/en/eu-charter#:~:text=The Charter of Fundamental Rights of the European Union (CFREU,the scope of EU law. (accessed Aug. 07, 2023).

[98] NCSC, “Which sectors and organizations are covered by the NIS2 directive?” https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/welke-sectoren-en-organisaties-vallen-onder-de-nis2-richtlijn (accessed Sep. 05, 2023).

[99] NIST, “Standards for Security Categorization of Federal Information and Information Systems,” *FIPS PUB 199*, no. February. NIST, p. 9, 2004. doi: 10.1016/b978-159749116-7/50032-9.

[100] ANSSI, “Active-Defense Cybersecurity for Industrial Control Systems.” ANSSI, Paris, pp. 1–6, 2012.

[101] Wikipedia, “Digital transformation,” *Wikipedia*. https://en.wikipedia.org/wiki/Digital_transformation (accessed Oct. 30, 2022).

[102] D. L. Rogers, “The Digital Transformation Playbook: Rethink Your Business for the Digital Age.” Columbia Business School Publishing, 2016.

[103] BZK, “Grondwet voor het Koninkrijk der Nederlanden.” pp. 1–68, 2008. [Online]. Available: http://deeplinking.kluwer.nl/docid/inod3c86b101d4fdbda1269a38a81dccc70a

[104] M. Porter, “Competitive advantage - creating and sustaining superior performance.” The Free Press, New York, 1985.

[105] Wikipedia, “Value chain Firm-level,” 2020. https://en.wikipedia.org/wiki/Value_chain (accessed Apr. 26, 2020).

[106] NATO, “NATO Interoperability Standards and Profiles, VOLUME I,” *NATO*. https://nhqc3s.hq.nato.int/Apps/Architecture/NISP/volume1/index.html (accessed Jan. 08, 2023).

[107] B. MAP and M. J. W. P‘t Hart, *Openbaar Bestuur– Beleid, organisatie en politiek*. 2011.

[108] Wikipedia-Community, “Enterprise resource planning,” *Wikipedia.org*, 2023. https://en.wikipedia.org/wiki/Enterprise_resource_planning (accessed Aug. 13, 2023).

[109] T. Gaidosch, F. Adelmann, A. Morozova, and C. Wilson, *Cybersecurity Risk Supervision*, vol. 19, no. 15. 2019. doi: 10.5089/9781513507545.087.

[110] D. Forscey, J. Bateman, N. Beecroft, and B. Woods, “Systemic Cyber Risk: A Primer.” pp. 1–27, 2022. [Online]. Available: https://carnegieendowment.org/files/Bateman_et_al_Cyber_Risk_final.pdf

[111] Wikipedia, “Cloud Computing,” 2020. https://en.wikipedia.org/wiki/Cloud_computing (accessed Aug. 30, 2020).

[112] S. Imran Akhtar, A. Rauf, H. Abbas, and M. Faisal Amjad, “Inter Cloud Interoperability Use Cases and Gaps in Corresponding Standards,” *Proc. - IEEE 18th Int. Conf. Dependable, Auton. Secur. Comput. IEEE 18th Int. Conf. Pervasive Intell. Comput. IEEE 6th Int. Conf. Cloud Big Data Comput. IEEE 5th Cybe*, no. August, pp. 585–592, 2020, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00103.

[113] ISO/IEC, “ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary,” *October*, vol. 3, p. 38, 2014, [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=42103

[114] Council of the European Union, “Information Assurance Security Guidelines on Network Defence (IASG 4-01).” Council of the European Union, pp. 1–33, 2015.

[115] Rijksoverheid, “Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie,” pp. 1–7, 2013, [Online]. Available: http://wetten.overheid.nl/BWBR0033507/2013-06-01

[116] Wolters Kluwer, “Escalation factors (Bowtie Risk Assessment),” *Wolters Kluwer*, 2024. https://www.wolterskluwer.com/en/solutions/enablon/bowtie/expert-insights/barrier-based-risk-management-knowledge-base/escalation-factors (accessed Jan. 17, 2024).

[117] Rijksdienst, “Besluit CIO-stelsel Rijksdienst 2021,” no. 62488. Staatscourant, pp. 1–21, 2021.

Glossary

ATO/IATO:	(Interim) Approval To Operate. Issued every three years by BC/BA (earlier for intervention). [11]
ABDO	"Algemene Beveiligingseisen voor Defensieopdrachten." Private sector companies that handle special information must comply with the security requirements. [75]
Accreditation:	Formal authorization and approval of special-information processing (article 1). [11]
ACM:	Autoriteit Consument en Markt. [54]
Agility:	Focused on effectively and decisively anticipating or responding to opportunities and threats, internal or external, to the Dutch Military, thereby (within the legislation framework) actively giving space to and stimulating bottom-up initiatives and innovation. [7]
AIVD:	"Algemene Inlichtinen en VeiligheidsDienst."
AP:	"Autoriteit Persoonsgegevens." [54]
Architecture regulation:	"determines what people can and cannot do aimed at changing the behavior of users through (secure) design," [20] for example, speed bumps to prevent speeding.
Asset:	ISO defines an asset as an item, thing, or entity with potential or actual value to an organization. Hence, an asset for which a party requires protection. [85]
Assets:	Information & Operational Technology (IT & OT) or cloud-based assets. [97]
BA:	"Beveiligings Autoriteit."
BC:	"Beveiligings Coordinator."
BOD:	"Board of Directors." One-tier governing body consisting of executive and non-executive directors. [19]
Boundary conditions:	Determined by conditions such as the (security) regulation framework, available financial, human, social, and technological resources, and implementation timeframe.
CER regulation (additional to NIS2):	Focuses on protecting public and private organizations against physical risks, such as the consequences of (terrorist) crimes, sabotage, and natural disasters. The European Commission adopted the CER regulation at the end of 2022. [95]
CIA:	The reliability aspects for Confidentiality, Integrity, and Availability.
CIO:	Chief Information Officer. The tasks are laid down in the 'Decree CIO structure civil service 2021'. [114]
CITV	"Commissie Toezicht op de Inlichtingen- en Veiligheidsdien." It was established based on the Wiv. [57]
Combat cloud:	Model for enabling ubiquitous, convenient, on-demand network access to a shared pool of sensors, navigation systems, weapon platforms, and C2 functions (aim: force multiplier for shrinking forces). [41]
Control frameworks:	The Dutch military is bound by civil service (BIO) and NATO/EU frameworks. The BIO framework is high over and does not consider state actor threats, unlike the NATO/EU frameworks.
Controller:	Entity (party) that determines the why and the how for processing personal data (Article 4 GDPR).
Critical assets:	Critical cyber activities enabled by IT platform services processing critical information.
CRM:	Cyber Risk Management cycle: this entails identifying the critical assets, identifying and assessing their risks for the organization as a whole, defining acceptable risk levels (low-hanging fruit first), deciding ways (s) of handling risks, and designing and implementing cyber risk measures in all cyberspace layers, see section 2.2.2.

Digital transformation:	Refers to the adoption of digital technology by a company to improve business processes, value for customers, and innovation. [98] [99]
Direct Control PDCA cycle:	Direct (PLAN), Execution" (DO/ACT"), and Control (CHECK). [30] See APPENDIX D.
Due process:	Follows procedures providing not only predictability but also allows sufficient time and space for consultation and the consideration of particularly affected constituencies; it grants involved parties rights and obligations. [20]
Dutch military strategy:	The leading objectives align with the mission "to protect what is valuable to us" depicted by the Constitution (Article 97) [100] and laid down in the charter for the Kingdom of the Netherlands. [7]
Dutch military supervisors:	Inspecteur-Generaal Veiligheid (IGV), Directeur Militaire Luchtvaart Autoriteit (MLA), Commandant Korps Militaire Controleurs Gevaarlijke Stoffen (KMCGS), Inspecteur Militaire Gezondheidszorg (IMG), Functionaris Gegevensbescherming (FG) en Beveiligingsautoriteit (BA). [77]
E&F/HR&O:	Equipment Logistics & Finance / Human Resource & Organisation.
EAR:	Enterprise Architecture Civil service provides a coherent description of the organization and design of the information services and facilities of the Central Government. [52]
Efficient (good supervision):	Regulatory procedures are conducted with minimal wastage and promptness, efficiently minimizing the distortion of market transactions and reducing the compliance burden. [20]
ERP:	Enterprise Resource Planning is the integrated management of main business processes, often in real-time and mediated by software and technology. [105]
Escalation factors:	"Conditions that lead to increased risk by defeating or reducing the effectiveness of barriers," also called Defeating Factors or Barrier Decay Mechanisms. In other words, Escalation Factors create the holes in the Swiss Cheese Model of James Reason. [113]
FG:	Functionaris gegevensbescherming.
Governance (IS) regulations:	Directives (strategy level), policies and company standards (tactical level), and procedures and guidelines (operational level). [23]
Governance structures:	see APPENDIX E. [7]
Hybrid cloud:	A composition of a public cloud and a private environment, such as a private cloud or on-premises resources, remain distinct entities but are bound together, offering the benefits of multiple deployment models. [108]
ILT (Inspectie Leefomgeving en Transport):	Supervises providers of essential services (ESOs) that fall under the responsibility of the Ministry of Infrastructure and Water Management. [55]
Infosec Process data:	General IT Controls (GITC), Security Action Plans, Risk Register or Asset Ownership. [23]
Integral cybersecurity supervision:	Cooperating state, sectorial, and organizational supervisory bodies aimed at (trust in the) end-to-end security of IT platform services.
Integrated control cycles:	Integrally coordinated and executable governance levels (APPENDIX G).
Interoperability:	From the perspective of the intra-cloud, the ability of two systems or clouds to exchange and use information, use each other's computing resources, and use each other software services securely and seamlessly while ensuring security and privacy. [109]
IRM:	Integrated Risk Management. Concerns realizing opportunities and managing threats for performing military tasks, (change) goals we want to achieve compliant

	with legislation and regulations (compliance management), fitting the organization's wide diversity and coherence of the different functional areas/domains and organizational units. [7]
ISMS	Information Security Management System. A systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's information security to achieve business objectives. It is based upon a risk assessment and the organization's risk acceptance levels designed to treat and manage risks effectively. [110]
IT platform services:	an IT system (such as C4ISR) composed of cloud & asset-based network & user devices.
IT/IS governance:	APPENDIX C presents examples inspired by the IS governance Direct Control cycle. [90] [91]
IT:	Information Technology.
Managed services:	User equipment and back-end capabilities (NATO NISP standard), see APPENDIX J)
Mandated business owners:	Mandated by BOD executive directors.
Market-based regulation:	Relies on incentives and self-interest to steer behavior. This variant appeals to individual and organizational self-interest to achieve regulatory goals without formal regimes, for example, via subsidies or taxation. [20]
MCO:	Military Cyber Operations are Intelligence, Defense, and Attack activities in cyberspace (besides the "real world") to maintain freedom of action and /or create effects to achieve a commander's military goals. [3]
MIVD:	Militaire Inlichtinen en VeiligheidsDienst.
Multi-stakeholders:	IT platform service suppliers, owners, producers, and consumers. [8] General public (multi) stakeholder policy objectives of these regulatees are addressed by self-developed regulations. [20]
NATO AC/322-D/0048-REV3 (INV):	CIS Technical and implementation directive. [76]
NFV:	Network Functions Virtualization. Specific network functions are implemented in software running on generic hardware without specific machines, enabling the sharing and reuse of functionality. [43]
NISP:	NATO Interoperability Standards and Profiles. [103]
NSA:	National Security Authority. Responsible for the security of NATO and EU classified information from other international partnerships & treaties and to conduct periodic inspections. [7]
Off-premise:	Services that are managed by an external IT service provider such as KPN, NATO, or the public sector. [44]
On-premise:	Services that are internally managed. [44]
Operational data:	Collected from, for example, Security Information and Event Management (SIEM) or Identity access management (IAM) security (sub) systems. [23]
Organization:	The terms 'organization' and 'corporation' are identical in this thesis and used interchangeably.
OT:	Operational Technology systems are, for example, civil Supervisory Control And Data Acquisition (SCADA) systems or Programmable Logic Controllers (PLCs). [97]
Performance info:	Dashboarding/reporting on, e.g., Maturity and risk levels, Benchmarking or compliance. [23]
Principles & tasks:	see APPENDIX F. [7]

Process domains:	Represents the Dutch military's three core business processes/activities with responsible policy/design (strategy) and (coordination of) implementation roles (mandated by SG, CHoD, and CMDs/DIRs). See Table 11 in APPENDIX H. [7]
Processor:	Entity (party) that performs the data processing on the controller's behalf (Article 4 GDPR).
Public-Private Partnership:	PPP. Involves cooperation between one or more organizations from Public administration and the Private business community, working together towards agreed objectives. [104]
Random security tests:	Desk research (setup), acceptance tests (existence), or penetration tests (exploitation).
Random security tests:	Desk research (setup), acceptance tests (existence), or penetration tests (exploitation).
Random security tests:	Desk research (setup), acceptance tests (existence), or penetration tests (exploitation).
Regulatees:	Regulated parties such as addressed by the Dutch Corporate Governance Code. [19]
Risk (ISO):	The effect of uncertainty on objectives is usually expressed in terms of risk sources, potential events, their consequences, and their likelihood. [28]
Robustness:	Focused on the planned and efficient realization and management of tasks and assignments, compliance with laws and regulations, and preventing incidents. [7]
SAA:	Security Accreditation Authority. See EU, IA Security Guidelines on CIS Security Accreditation, IASG 1-01, 22 and 24 [111], NAVO, Guidelines for the security accreditation of communication and information systems (CIS), AC/35-D/1021-REV3, Section IV.1.11, [76] VIR-BI, artikel 3 Beveiligingsbeleid. [112]
SDN:	Software Defined Networking. Third parties can control network resources and their performance (Complementary to NFV). [43]
Sensemaking process:	Is backward-focused, forming reasons and understanding for past events. [31] [32]
Situational Awareness (SA):	Endsley points out that SA typically looks ahead and projects what is likely to happen to inform effective short-term decision-making processes. [31] [32]
Special information:	Information where access by unauthorized persons can have adverse consequences for the interests of the State, its allies, or one or more ministries. [11] [112]
Stakeholders:	Groups and individuals who, directly or indirectly, influence – or may be influenced by – the attainment of the company's objectives: employees, shareholders, other lenders, suppliers, customers, and other stakeholders. [19]
Standardization bodies:	Such as the International Standardization Organization (ISO), NIST, and NATO Security Committee (see also section 4.2). [27] [76]
Supervised party (regulatee):	Organization, person, IT (platform) owner, group, or other body on whose behalf a risk analysis is conducted.
Supervisory & Management Boards (SB/MB):	A two-tier governing body comprising a Management Board with executive directors and a Supervisory Board with non-executive directors. [19]
Systemic risks (with cascading effects):	The possibility that a single event or development (caused by the system, organizational design, or culture) might trigger widespread failures and adverse effects spanning multiple organizations, sectors, or nations. [25] [106] [107]
TBB category 1:	classification when confidentiality of information is classified: "Top Secret."
TBB category 2:	classification when confidentiality of information is classified: "Secret."
Te Beschermen Belang (TBB):	Four pre-defined categories of interests to be protected are aligned with the Dutch military regulations for the compliance management system, one of the IRM components. [7]

Threats:	ISO defines a threat as a potential cause for an incident that may harm organizations, assets, or cloud-based services and cannot be controlled (generally). [85]
TIB:	“Toetsingscommissie Inzet Bemachtheden”. [57]
Trust:	Defined as a necessary condition for realizing the expected benefits. [16]
Tw:	“Telecommunicatie wet.” Transposed from the EECC and the current ePrivacy Directives. [54]
uAVG:	“Uitvoeringswet Algemene Verordening Gegevensbescherming.” Adopted the GDPR. [63]
Value chain:	A collection of activities that are performed by a company to create value for its customers. As a result, the added value leads to a competitive advantage (Porter et al.). [101] [102]
Value-creation:	Expected value creation for the Dutch military core business processes (value chain) enabled by the provided IT platform services. See section 2.3.2.
Vulnerabilities:	ISO defines a vulnerability as a weakness in a (critical) asset or a sum of assets that one or more threats can exploit, and (proactive) steps should be taken to address it. [85]
Wbni:	“Wet bescherming netwerken en informatiesystemen.” Transposed from the NIS directive. [55]
Wiv:	“Wet op de inlichtingen- en veiligheidsdiensten;” forms the legal framework for the General Intelligence and Security Service (AIVD) and Military Intelligence and Security Service (MIVD). [57]
WPG:	“Wet Politie Gegevens.” One of the GDPR exceptions is processing personal data to prevent, detect, or prosecute criminal offenses. This 'police data' falls under a separate Police Data Act (WPG). [64] [65]
WRR:	“Wetenschappelijke Raad voor Regeringsbeleid.” Advises the Dutch government by providing evidence-based information on trends and developments that may impact society long-term. The Council must point out contradictions and anticipate problems at the earliest possible stage, identify problems related to significant policy issues, and propose policy alternatives. [49]
Wvo:	“Wet veiligheidsonderzoeken.” Regulates a security investigation of a person conducted before an employer appoints them to a position of trust. [67]

APPENDIX A

Guideline	Description	Additions of this research to the guideline
Guideline 1: Design as an Artefact	Design-science research must produce a viable artifact as a construct, a model, a method, or an instantiation.	Because the cybersecurity supervision model is a viable artifact, the research objective is a design science issue. Thus, this thesis follows the steps of the Hevner design science guideline.
Guideline 2: Problem Relevance	Design science research aims to develop technology-based solutions to important and relevant business problems.	The relevance of this research is that it assists organizations in developing a cybersecurity supervision approach to deal with the dynamics of cyberspace (changing environment). Additionally, this research provides a tailor-made cybersecurity supervision approach for the Dutch military.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.	The departmental Chief Security Officer (CSO: Dutch military BA) evaluated the cybersecurity supervision model by applying the tailor-made design steps to approve critical IT/OT. See also **E** in Figure 5.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.	See following Table 9, *Research contributions*, and **C** in Figure 5.
Guideline 5: Research Rigor	Design-science research relies upon applying rigorous methods in constructing and evaluating the design artifact.	See Table 10, Overview of used *analytical & empirical research methods,* and **C** in Figure 5.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.	The fast speed of innovation causes practical problems/challenges for the Dutch military cyber domain that necessitate the search (engineering cycle) for a possible solution. During the search, alternatives were examined and weighed to solve the problem/challenges; this is about the various applied concepts from the literature/*knowledge base*. The knowledge from the *knowledge base* covers cybersecurity theories, frameworks, and concepts; this knowledge is derived from theoretical research, industry standards, regulatory frameworks, legislation, and abstract expertise from field experts. See also **D** in Figure 5.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	The tailor-made design steps are presented to representatives of organizational Chief Security Officers and technical-oriented representatives of IT service suppliers. See also **E** in Figure 5.

TABLE 8 HEVNER ET AL. [8] DESIGN GUIDELINES EXPLAINED FOR THIS RESEARCH

	Research contributions (guideline 4 in Table 8 and C in Figure 5)
	The research contribution consists of both the design approach and the constructed model itself. No design approach in the knowledge base can serve as a tailor-made guideline and method for developing a cybersecurity supervision model (framework) for organizations. The cybersecurity supervision approach extends the Hevner design approach (consisting of generally applicable methods and techniques) for designing tailor-made cybersecurity supervision models applicable in other cyberspace sectors presented in Figure 1. The constructed model itself provides a solution to the Dutch military's organizational problem/challenge (business need) for dealing with cyberspace dynamics. The dynamics concern the rapid pace of innovation, which causes practical problems/challenges that can affect the Dutch military organization and its staff via targeted social engineering or IT/OT hacking activities by, for example, state actors. Therefore, this research examined how cybersecurity supervision can support dealing with the dynamics of cyberspace. The solutions came in the form of analysis and the design of the final cybersecurity supervision model.

TABLE 9 RESEARCH CONTRIBUTION [8]

Method	**Research Rigor (guideline 5 in Table 8 and C in Figure 5)**
Desk research	The Desk research method helps better understand the problems/challenges for the Dutch military environment. Searching for a solution to the identified problems/challenges requires knowledge from different disciplines to investigate the issue. In addition to the technical area, this also involves exploring knowledge areas such as public administration/governance, supervision, business management, economics, and legal sciences. In addition, this research used research papers and documentation from knowledge bases within and outside the Dutch military, including open sources such as Wikipedia.
Semi-structured interviews	Representatives of Departmental and organizational Chief Security Officers CSO (BA/BC), users, and IT service suppliers have contributed via the involvement of the development of the Dutch military supervisor (BA/BC) "eight-step approval process" of critical IT/OT platform services. Reports of meetings on the information collection for assessing fourteen critical IT platform services based on the "eight-step approval process."

TABLE 10 OVERVIEW OF USED ANALYTICAL AND EMPIRICAL RESEARCH METHODS [8]

APPENDIX B

"Due to the increasing interdependence of ICT and business operations, the organizational units will claim an increasingly prominent role in management. Information management is becoming increasingly important and, therefore, embedded in organizational units. On the other hand, ICT will increasingly be outsourced to external service providers. We see these trends reflected in Gartner 's IS Lite model." [28]
"This poses a major challenge for organizations because both information management "managing demand" and outsourcing "managing delivery" require an increasingly higher level of professionalism, while the execution must increasingly be managed within the regular operation." [28]
"To meet this need, ICT service organizations have set up a Demand-Supply Organization (DSO) with a central ICT management function that coordinates all processes at a strategic and tactical level. The control side of Information Management is thus evolving in larger organizations towards ICT management (ICT governance) and also integrates the Enterprise Architecture function (ICTRA). A business strategy, Information strategy, and ICT strategy are integrated into the strategic management processes of the organization. This development also affects the most important ICT roles, as shown iin Figure 20 below." [28]

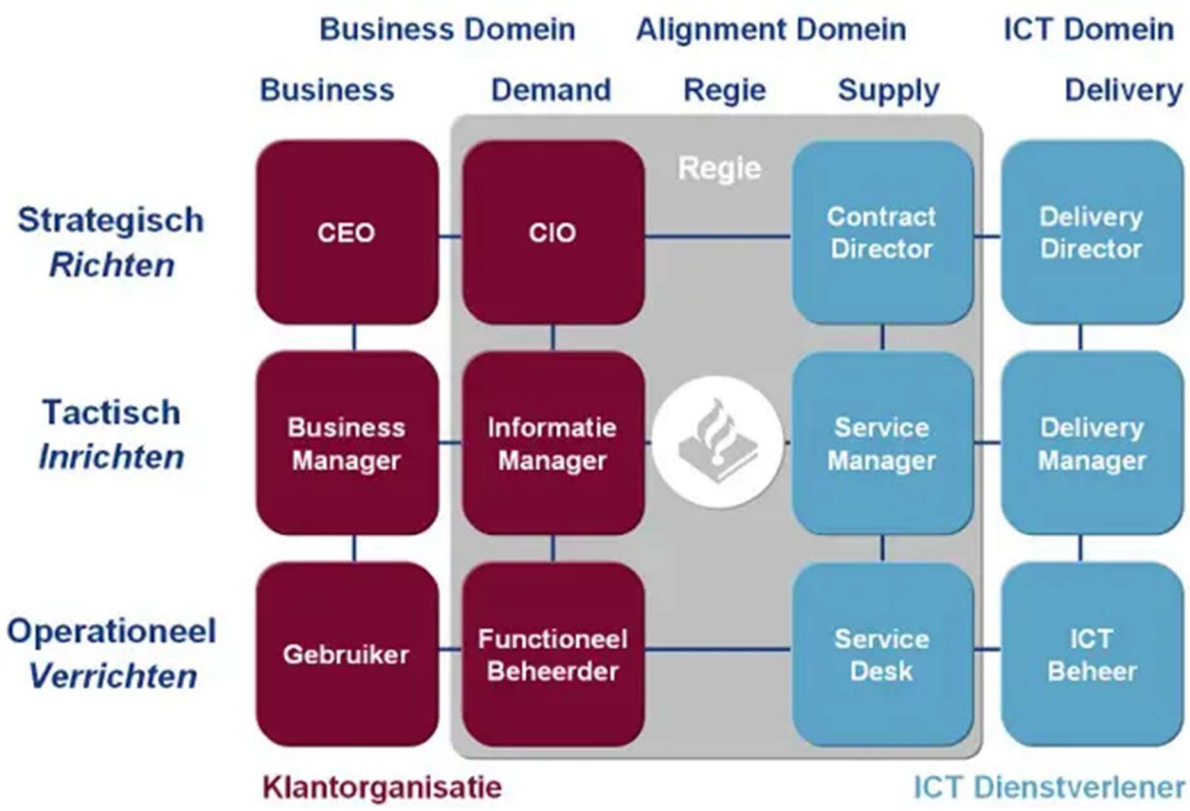


FIGURE 20 BUSINESS - IT RELATIONSHIP

The model distinguishes three control domains (Mapped to the socio-technical and technical layers displayed in Figure 3 in the introduction chapter) [28] and relates the domains to the governance, as shown Figure 20 and Figure 21:

- Business operations (Business domain) - This domain contains regular business operations with all its facets, such as people, resources, processes, etc.
- Information & communication provision (Information domain) - This domain specifically concerns information as a supporting resource for the business domain. Here, the demand

for information provision from the business domain is translated into a demand for ICT (technology)."

- Information and communication technology (ICT domain) - This domain explicitly concerns developing and exploiting ICT (technology).

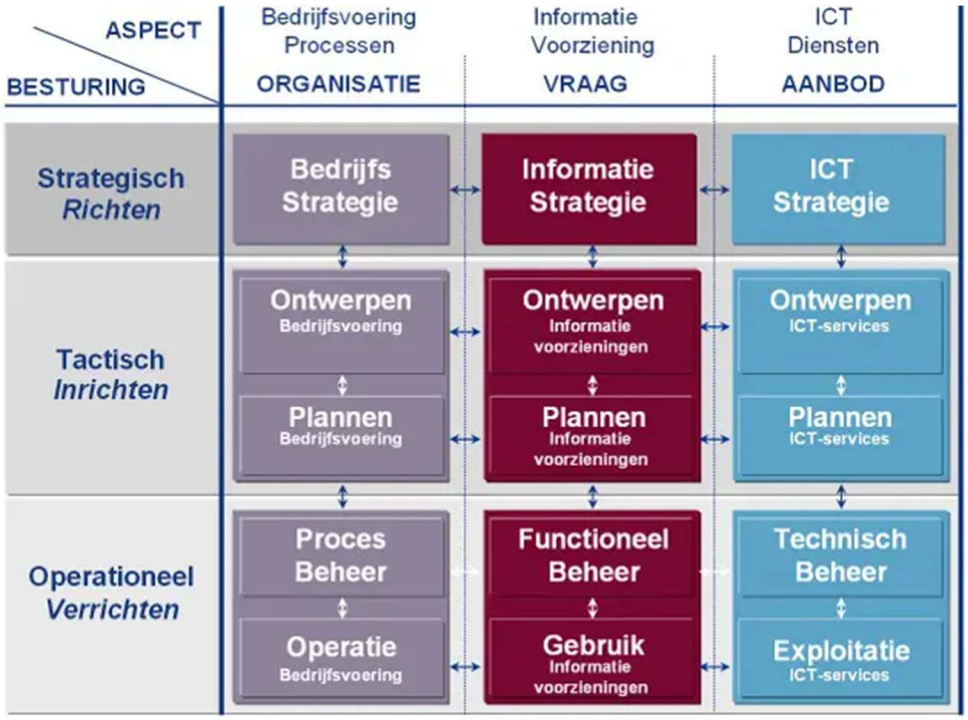


FIGURE 21 BUSINESS, INFORMATION, AND ICT DOMAINS RELATED TO THE GOVERNANCE

"On the vertical axis, we see the control levels as we know them from the control frame: strategic (aiming), tactical (structure), and operational (executing). This model is derived from the Strategic Alignment model by Henderson and Venkatraman (IBM, 1993)." [28]

APPENDIX C

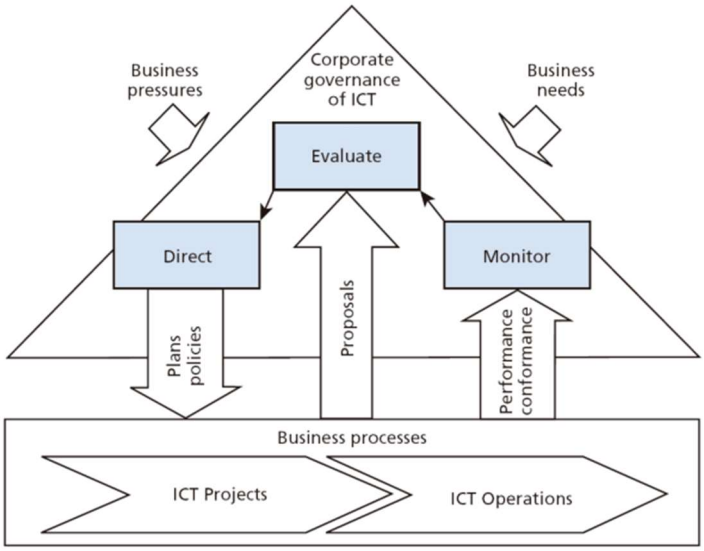


FIGURE 22 MODEL FOR CORPORATE GOVERNANCE OF IT (ISO38500) [93]

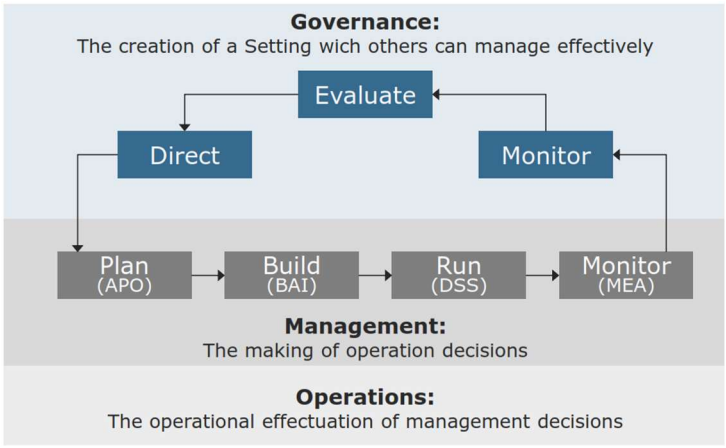


FIGURE 23 ISACA IS GOVERNANCE [94]

The BOD members (strategic level) are responsible for creating a setting that other decision-makers at the tactical (structure) and operational (operations) levels can manage effectively. (source ISACA).

APPENDIX D

The direct-control cycle consists of three actions: Direct, Execution, and Control. Regarding the PDCA cycle, the PLAN step concerns the Direct actor, the DO/ACT step concerns the Execution actor, and the CHECK step concerns the Control actor. The PDCA steps are visualized in Figure 24.

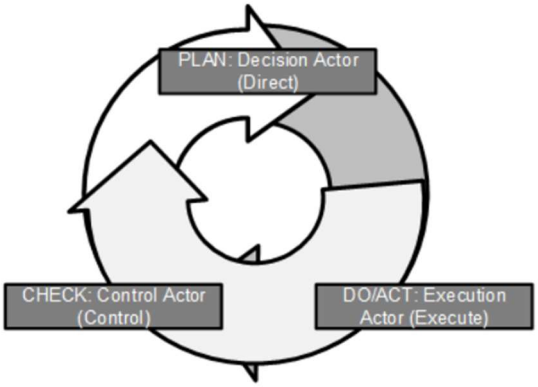


FIGURE 24 THE PDCA CYCLE ON DIRECT CONTROL CYCLE OF VON SOLMS & VON SOLMS BASED ON TEWARIE [36]

Direct actor: The senior executive and non-executive BOD members (strategic level) define the organization's general direction and security strategy.
Senior and middle management (tactical level) converts these objectives into quantifiable key performance indicators (KPIs) following information security management and policy practices.
The direct actor seeks to provide direction on the information security goals and implement an appropriate plan. Plans, strategies, resource allocation, and many other aspects of risk management can all be affected by changes in direction.

Execution actor: The directives are translated into policies and from policies into procedures by lower-level management (executive level). The operational/executive departments are responsible for executing the roadmap/plans.

Control actor: Collection of feedback. The operational/executive departments (executive level) report to their tactical managers (tactical level) to check if the procedures are adequate. Tactical management uses this feedback and their measurable KPIs as input for the BOD members (strategic level). The goal is to check the effectiveness of the directing process. With the gathered information, the BOD members can evaluate the progress of the information security management system.
For information security governance, the results generated by the Direct-Control Cycle are essential feedback for the management program. Furthermore, the strategic level can use this feedback to change its strategy to get the desired result. [29] Therefore, direct (PLAN) and control (CHECK) actions are the main focus of information security governance at the strategic level. The DO/ACT steps are the main focus for the management at the operational/executive level (operational actor) and report to their managers at the tactical/structure level.

Note that the strategic, tactical, and executive levels correspond to the strategic (why/what?), structure (how?), and operations (result?) levels of Figure 3, respectively.

APPENDIX E

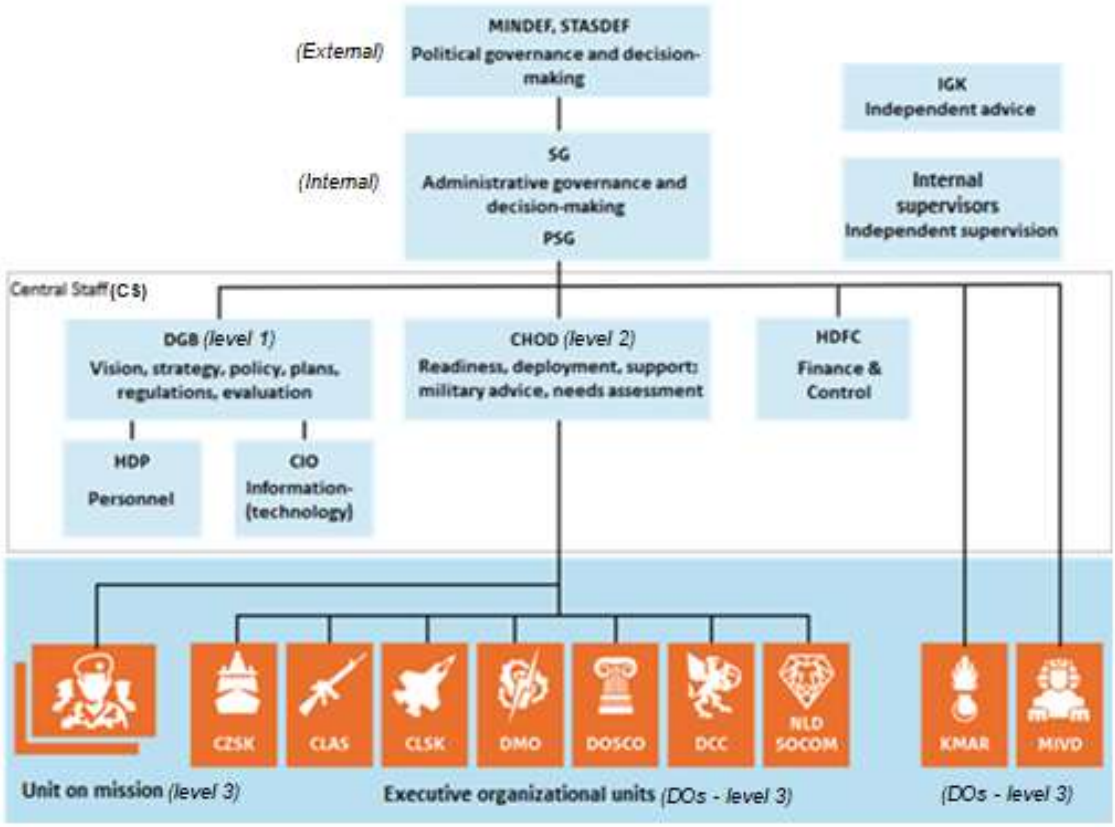


FIGURE 25 THE DUTCH MILITARY ORGANOGRAM

Central Staff (CS): is based in The Hague and develops the Defence policy. In broad terms, it directs the Ministry of Defence's activities, allocates the Defence budget, and monitors Defence spending. The commanders of the Services of the armed forces ensure that Defence policy is implemented. The Central Staff also advises the Minister of Defence (**MINDEF**) in his or her capacity as a member of the Cabinet. MINDEF is responsible for the overall Defence policy. The Secretary-General (SG) is responsible for civil leadership duties. The Chief of Defence (**CHoD**) is the most important military adviser to MINDEF and supervises the commanders (**CDT/DIR**) of the Navy, Army, Air Force, Joint Support Command, Defence Materiel Organisation, Defence Cyber Command and Special Operations Command.

CHoD: holds the highest military position in the Dutch military organization. In this position, he is the most senior military adviser to MINDEF. On behalf of the minister, he is responsible for preparing and executing military operations by the Netherlands armed forces. From his position in the CS, the CHoD directs the Navy, Army, and Air Force activities. He is also in charge of the Royal Netherlands Marechaussee, when it is operating under the responsibility of MINDEF. The CHoD is the military adviser to MINDEF when decisions are made about Defence policy. He also advises about any future military capabilities and deployment.

Royal Netherlands Navy (CZSK): The fleet, navy personnel, and marines of CZSK are deployed worldwide to ensure security at and from the sea. In addition, CZSK takes part in crisis management operations at home and abroad and provides humanitarian assistance and disaster relief. CZSK is the oldest of the 4 Services of the Dutch military (Netherlands armed forces).

Royal Netherlands Army's (CLAS) land operations contribute to freedom, security, and prosperity in the Netherlands and abroad. The CLAS can perform its tasks thanks to its professional and well-trained military personnel. They push on where others stop. They conduct combat operations under

extreme circumstances, provide humanitarian aid, and lend support during disasters.
Royal Netherlands Air Force (CLSK): is a modern, high-tech armed forces Service that contributes to peace and security globally. For this purpose, it has highly qualified personnel, aircraft, helicopters, and other weapon systems.
Royal Netherlands Marechaussee (KMAR): safeguards the security of the State, both in the Netherlands and further afield. It is deployed globally at locations of strategic importance: from royal palaces to the external borders of Europe and from airports in the Netherlands to theatres of war and crisis areas worldwide. The KMAR is deployable for security at home and abroad, especially when going is tough.
Joint Support Command (DOSCO): supports the entire Dutch military. This support concerns food, health care, building management, exercise areas, education, and personnel services. By taking care of these matters, Joint Support Command enables the Navy, Army, Air Force, and Marechaussee to focus on their principal tasks, namely operations at sea, on land, and in the air, to promote peace and security.
Defence Materiel Organisation (DMO): ensures that military personnel have modern, robust, and safe material to work with. The DMO is involved in procuring, maintaining, and selling material.
Internal supervisors: naast de toezichthoudende rol van de HDFC en de CIO beschikt Defensie over de volgende interne toezichthouders (conform het Algemeen Organisatiebesluit Defensie): de Inspecteur-Generaal Veiligheid (IGV), de Directeur Militaire Luchtvaart Autoriteit (MLA), de Commandant Korps Militaire Controleurs Gevaarlijke Stoffen (KMCGS), de Inspecteur Militaire Gezondheidszorg (IMG), de Functionaris Gegevensbescherming (FG) en de Beveiligingsautoriteit (BA). [77]
BA: The director of Operations and Evaluation of the DGB in his delegated role as National Security Authority; The Security Authority (BA) draws up the Defense Security Policy (DBB) on behalf of the Secretary-General (SG) and supervises its implementation. The DBB describes the responsibilities and tasks of the chain partners involved in Integrated Security, consisting of Personnel, Physical, Information, and Industrial Security.
Additionally, with the 'Decree CIO structure civil service 2021' and the relation between information security and integrated security, it is necessary also to update the formal basis of the 'Decree BVA structure civil service 2021' and to standardize and describe the functions of the departmental security authority and the National Security Authority. The BVA system decision is a further elaboration of the legislation and regulations. It gives practical substance to the integral security system, the BVA consultation, and the functions and tasks of the BVA Central, the BVA of departments, and the BVC of service units.

Directeur-Generaal Beleid (DGB): develops the vision and strategy for modern and future-proof armed forces and is charged with integral responsibility for international policy. The DGB is also responsible for providing official support and advice to ministers. The DGB is accountable for drawing up integral and implementable defense-wide policy (including internal regulations and frameworks) and its evaluation and for defense-wide plans. The DGB's integral policy task includes operations, international cooperation, personnel and military healthcare, equipment, real estate, facilities, sustainability, governance, security, purchasing and divestiture, information provision, information technology (including defensive cyber and data), and security.
HDP: taking into account the instructions of the Minister of Defense (MOD), he is charged with the defense-wide responsibilities for being an employer, which in any case includes the responsibility that follows from the Decree on organized consultation in the Defense sector.
Hoofddirecteur Financiën en control (HDFC): is the Defense group controller responsible for the functional domain of finance and control. HDFC prepares the draft budget, the supplementary budget, and the annual report

Chief Information Officer (CIO)[94]: is functionally managed by the SG (In line with the Central Government CIO System Coordination Regulations). Due to the integrality of vision, strategy, policy, and plans, the CIO is part of the DGB and contributes to and implements the DGB's business plan. The CIO advises the official and political leadership on the organization's information policy and strategic issues and the IT, data, and cyber (defensive) implications of (proposed) legislation and regulations, policy and implementation processes, and investments. Chief Information Security Officer (CISO) and Chief Data Officer (CDO) fall to the CIO.

[94] CIO (Chief Information Officer): The tasks are laid down in the 'Decree CIO structure civil service 2021'. [117]

APPENDIX F

The Dutch Military Vision 2035 [95] outlines the threats and developments in the world around us. The speed of changes in the environment of the Dutch Military requires a high degree of adaptation and innovative capacity. When governing the Dutch military, striking a good balance between robustness[95] and agility[96] is important; this is an important responsibility and a challenge for all BOD members. A good balance is relevant for the present and future of the Dutch Military.[16] The directive further elaborates this vision in governance principles for behavior - derived from the Dutch Military Code of Conduct - and for working methods. Our (exemplary) behavior as directors and as staff members of directors are crucial for the result. The corporate governance principles concerning the working method are: [16]

1. Clear assignment of tasks, responsibilities, and authorizations (TVB);
2. Governance with transparent and up-to-date information (historical, planning, and predictive data (scenarios));
3. Policies, plans, commands, integral and executable;
4. Tasks and responsibilities in balance with authorizations and available resources;
5. Simplify processes;
6. Integral risk management (incl. compliance);
7. Simplifying regulations (the 'what' from the point of view of the regulations, not the 'how').

The Dutch military Code of Conduct matters about solidarity, safety, trust, and responsibility. The corporate governance principles concerning behavior are: [16]

1. Working together in the interest of the Dutch military as a whole;
2. Providing responsibility, taking responsibility (ownership; entrepreneurship), and accountability;
3. Work safely;
4. To be transparent;
5. Being trustworthy;
6. Providing confidence;
7. Be risk aware;
8. Work with awareness of the environment.

Within the context of the Dutch military vision and mission "*to protect what is valuable to us*"" [16], the corporate governance tasks are:

1. Determining the joint mission (about the constitutional tasks), values, and rules of conduct for the Dutch military organization;
2. The Dutch military actively looks ahead, developing scenarios for developing the organization and the capabilities required for this and converting this into a vision for the future. The vision must be periodically adjusted to prepare the necessary decisions about and for Defense in good time given (inter)national developments. It is up to the government to make decisions about this and to make the necessary financial resources available. Subsequently, integrally coordinated and executable policy objectives, the associated plans, and the budget drawn up;
3. The Dutch military organizes both the governance and executive processes and the implementation of projects, everything necessary to achieve the objectives. Objectives concern

[95] Robustness: focused on the planned and efficient realization and management of tasks and assignments, compliance with laws and regulations, and preventing incidents. [16]

[96] Agility: focused on effectively and decisively anticipating or responding to opportunities and threats, internal or external, to the Dutch Military, thereby (within the legislation framework) actively giving space to and stimulating bottom-up initiatives and innovation. [16]

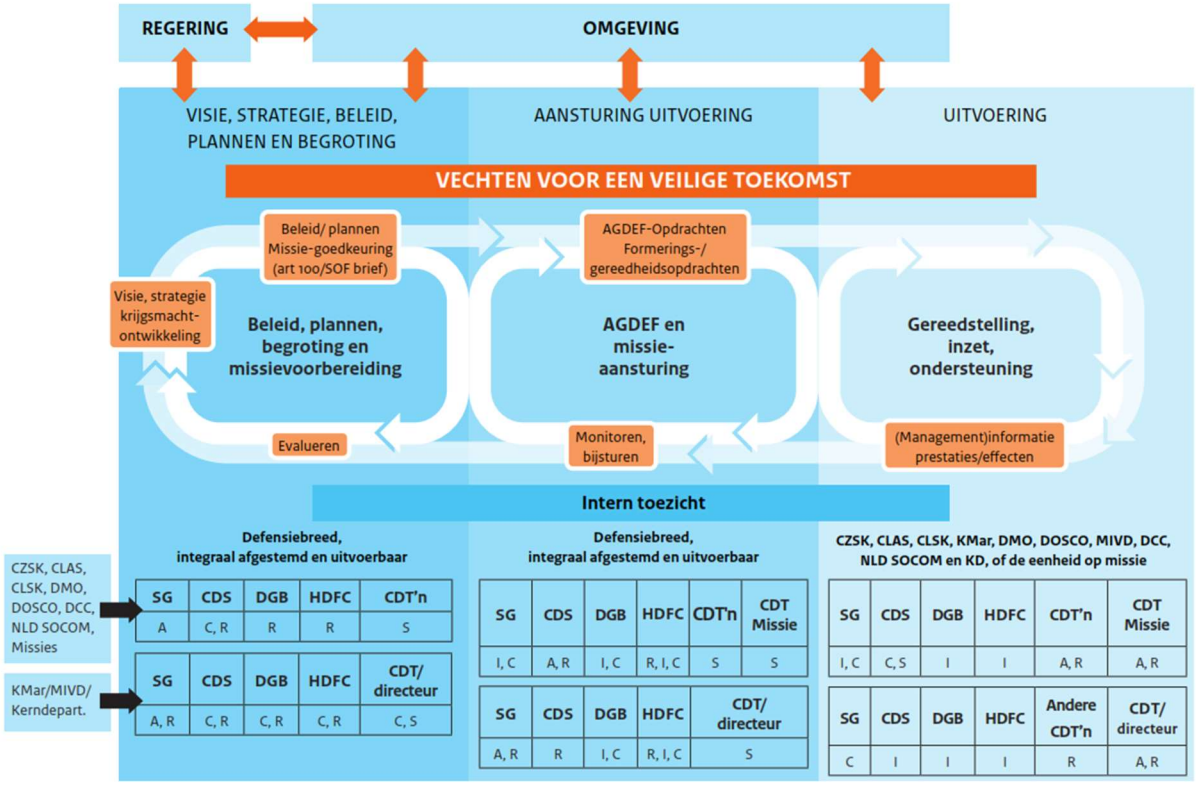
the performance (output) and the intended effects (outcome). Key Performance Indicators (KPIs) are defined target values based on which the degree of target achievement can be tracked.

4. The Dutch military management task, i.e., facilitating and supporting employees with straightforward tasks, responsibilities and authorities (TVBs), objectives, and the necessary resources. In addition, training and coaching so that they can develop through their work, achieve the set goals as independently as possible and accomplish tasks and goals.
5. The Dutch military coordinates tasks both vertically (hierarchically) with assignments and allocating resources (personnel, financial, equipment) and facilitates horizontal self-coordination between the executive organizational units at the operational level. The tasks also include proactively facilitating bottom-up innovation and initiatives at the executive administrative units for the renewal of the Dutch military.
6. Monitoring and directing whether policy objectives/tasks/assignments are being achieved using interim effect measurements and whether legislation and regulations are being complied with, where necessary, proactively adjust, set priorities, or adjust assignments and policy goals. Independent internal and external supervisors also play an essential role in their findings and advice.
7. The Dutch military is accountable for realizing set objectives/assignments, for good stewardship of entrusted people and resources, and whether the powers granted have been exercised with integrity. Accountability applies internally to the Dutch military and the ministers to parliament.

Note (task 6): for compliance with laws and regulations, the executive directors (CDT and DIR) have a compliance management system, one of the Integrated Risk Management (IRM) components. With transparent and up-to-date management information, executive directors (CDT and DIR) provide insight into the realization of the implementation and then report to the BOD (SG or CHoD) about any decision points that fall outside the scope of the assignments issued.

APPENDIX G

The Dutch military governance model with three governance levels (1, 2, and 3) is chosen to provide insight into how the Dutch military governs its organization. For each governance level, Figure 26 specifies which officers are responsible (R), Accountable (A), Supportive (S), Consulted (C), or Informed (I), the main points of which are explained and visualized below.



R:	Responsible to the accountable officer for results (primary action holder); responsible for realizing tasks.
A:	Final responsibility (decision maker): The person who is ultimately responsible for the final result of the organizational unit and who takes the decisions at the relevant management level. In a combination of Accountable (A) and Responsible (R), the R is, in practice, commissioned to a board of directors or a staff department.
S:	The person who supports the responsible and/or consulted officer with advice, knowledge, and expertise.
C:	Two-way street: The person who must be consulted before decision-making is mandatory because of their essential voice in the final decision-making. The approach here is that the responsible and consulted officers agree in good consultation; if the responsible and consulted officers cannot agree, this will be submitted to the accountable officer.
I:	One-way street: The person who must be informed using current (management) information.
Note the internal supervisor role (2.2.3) overseeing each cycle. Regardless of the organizational suspension, the Dutch military internal supervisors have an independent position and direct access to the SG. Therefore, these supervisors play an essential role in the quality of task performance by the management team and compliance with external and internal regulations.	

FIGURE 26 DUTCH MILITARY GOVERNANCE MODEL INCLUDING THE RASCI TABLE [16]

1. Vision, strategy, policy, plans, and budget (defense-wide): SG(A) is ultimately responsible for vision, strategy, policy, plans, and budget in preparation for political decision-making. Vision, strategy, integrated policy (including internal regulations and framework), and plans are drawn up by the DGB(R). The HDFC(R) draws up the budget and Finance and Control (F&C)-related internal regulations and frameworks. The CHoD (Consulted by DGB and HDFC) contributes to this (R) with integral advice on the development of the armed forces, statements of needs for (military) capacities, and the feasibility test of policy proposals, regulations, and frameworks (within and for the organizational units falling under him). This policy applies to the KMar and MIVD plans are partly established interdepartmentally, under the responsibility of the SG, with advice from the legal affairs department (DJZ), among others. Before interdepartmental (political) decision-making, the (financial)

suitability and feasibility are tested within the Dutch military. The CHoD is also responsible (R) for preparing all deployment operations, subject to the instructions of the Minister. CDT/DIR (S) of CZSK, CLAS, CLSK, KMar, DMO, DOSCO, MIVD, DCC, and NLD SOCOM contribute with knowledge and expertise from their organizational units.

2. Integral governance of the implementation (defense-wide): The SG (A and R) governs the KD, the KMar, and the MIVD integrally by interdepartmental coordination and is subject to operational control of the KMar by other authorities. The CHoD (A and R) integrally controls CZSK, CLAS, CLSK, DMO, DOSCO, DCC, and NLD SOCOM, or in the case of deployment, the Dutch commander on a mission. Integral management of the implementation is understood to mean management aimed at all factors relevant to the assignment/task within the given frameworks, guidelines, and authorities. Integral governance of the implementation focuses on the following elements:

i. Operationalize policy (including internal regulations and frameworks) and plans in integrally coordinated and executable assignments for the executive organizational units, focusing on intended performance and effects. This results in Defense integral Preparation Instructions (AGDEF) for the executive organizational units, which the SG determines;
ii. Structure (setting up) and govern the executive processes for all process domains (operations, personnel, equipment, real estate, etc.) for the executive organizational units falling under the SG and CHoD, respectively. The design and management of F&C processes is an exception; HDFC is responsible for this within the frameworks of the Accountability Act and the FEZ Task Decree, as well as the frameworks and instructions given by the SG and in coordination with the CHoD. At the KD, the KMar and the MIVD are used as much as possible for non-operational and defense-wide processes;
iii. Directing the implementation at the SG and CHoD, respectively, executive organizational units (monitoring whether the intended performance and effects are realized, support, prioritize, and adjust where necessary, based on current information management information), with deviations from the AGDEF and/or the budget for decision-making, be submitted to the SG.

3. Execution (per executive organizational unit): the commanders/directors (A and R) of CZSK, CLAS, CLSK, KMar, DMO, DOSCO, MIVD, DCC, NLD SOCOM, and the KD integrally manage the implementation within their organizational units, including mutual (operational) support from JODs and assortment managers. Regarding deployment, the Dutch CDT is in command of the unit; with this, the CDT/DIR (A) complies with the AGDEF assignments, defense policy, and laws and regulations. They have a compliance management system for compliance with laws and regulations, one of IRM's components (see Appendix E). With transparent and up-to-date management information, they provide (R) insight into the realization of the implementation and report to the SG and CHoD, respectively, any decision points that fall outside the scope of the assignments issued or bottlenecks in the area of compliance (SG and CHoD: I and C, respectively) at decision points or bottlenecks).
In governing the Dutch military, the realization of government policy and its results and effects are central. The Dutch military achieves this by ensuring the governance levels are well aligned. Figure 26 shows the tuning approach using three integrated control cycles for each governance level.

Alignment with the governance levels using an integrated overall control cycle comprising the three control levels for each sub-control cycle:

i. The left-hand cycle concerns the formation of a vision and strategy, the integrated policy and plans based on this and its incorporation into the budget, and the interdepartmental preparation of missions;
ii. The middle cycle concerns the management of the implementation with the AGDEF, the management of missions, and then the management of the implementation (monitoring and prioritizing);

iii. In addition, each operational organizational unit has a control cycle, which must achieve the intended performance and effects in mutual coordination.

Applying a planned BPB cycle, as illustrated in Figure 27, is important for the Dutch military to manage robustly. However, not everything that happens or should happen in the Dutch Military benefits from a systematic approach alone. Sometimes, insufficient information or knowledge is available to make a good plan. For example, if it is not yet known which solutions solve which problem, with which action a goal is achieved, or how to use an opportunity best. For the governance model, directors must consciously create space at every level (capacity and budget planned) for new initiatives, innovation, experimentation, and scaling up in case of success. [16]

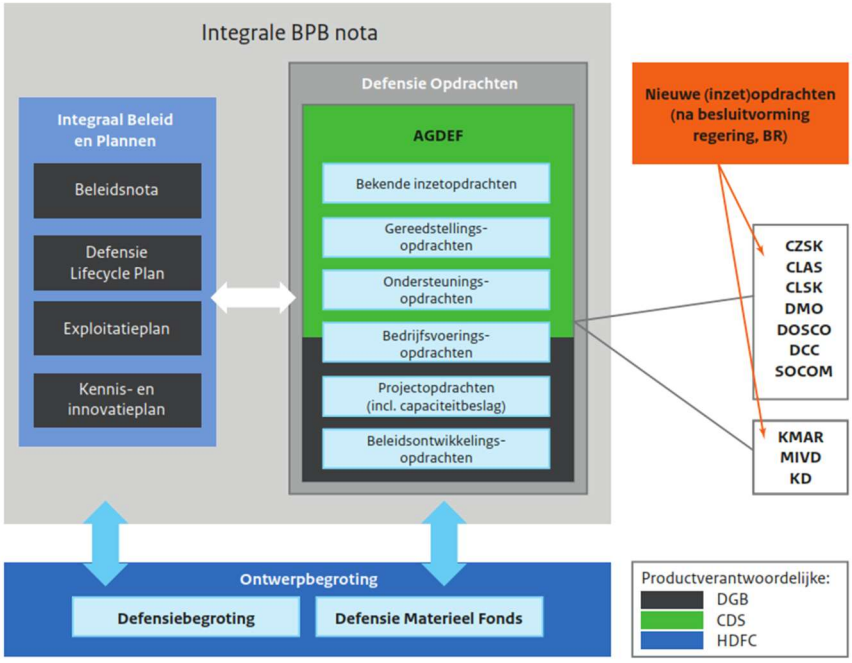


FIGURE 27 INTEGRAL POLICY, PLANS, AND BUDGET (BPB) NOTE [16]

APPENDIX H

Table **11** lists the Dutch military process domains and represents the Dutch military's three core business processes. See section 2.3.2. [16]

Process domains	Processes
Operations (Exercise / Readiness)	Deployment Exercise / Readiness
Finance & Control (F&C)	Samenstellen/verantwoorden begroting Realiseren begroting Beheren financiële stamgegevens/contracten
Governance	Exercise / Readiness Beleid en plannen Coördinatie allocatie Bedrijfsvoeringsaspecten (CM, IRM, Evaluatie, PBG, etc) Project-, programma-, portfolio management
Equipment & Logistics (E&L)	Chain logistics System logistics
Physical living environment & Real estate	Environmental management Environment planning Obtaining consent ('permits') Real estate
Durability	Environmental Energy Circularity
Facilities	Facilities
Movements & Transport	Traffic Transport Movements Mobility
Human Resource & Healthcare	Human Resource Management Military Medical Healthcare
Purchase and Divestiture	Purchase Divestiture
Information	Generieke informatievoorziening (IV) Documentaire informatie Privacy (AVG/WPG) Geografische informatie
Security	Beveiliging algemeen en organisatie Personele beveiliging Fysieke beveiliging Informatiebeveiliging Special Access Program
Safety	Safety (physical) Safety (social/integrity)
Legal Affairs	Legal Affairs
Communication	Communication
Supervision	Security Authority (BA) Privacy Data Protection Officer Safety Inspection Officer Military Healthcare Inspection Military Aviation Authority Corps of Inspectors of Military Hazardous Materials

TABLE 11 PROCESS DOMAINS AS ELEMENTS OF THE DUTCH MILITARY'S THREE CORE BUSINESS PROCESSES. [16]

APPENDIX I

Process management in the Dutch military is mainly divided into three roles:

1. Policy responsible (including internal regulations and framework),
2. Design responsible (including the design of processes in information systems),
3. Implementation responsible (including data quality in information systems).

These roles must be determined per process domain [16] and are assigned to an official, i.e., (1) a Policy Manager for each process domain at the DGB (SG ultimately responsible), (2) a Coordinating/ Implementation Process Manager (CHoD responsible), and (3) an executive organization manager (CMD/DIR of DO/subunits responsible). DGB/DBE is responsible for this process management system in the Dutch military and draws up instructions. The CHoD is responsible for designing processes in an information system and often requires specific knowledge and expertise. The CHoD can mandate this task to a commander (CMD)/director (DIR) of an executive organizational unit if this unit is the main user of the information system and/or if this organizational unit has the required capacity, knowledge, and expertise.

In process management, the integrality between the various process domains is (horizontal), and the coherence within the processes (vertical) is of great importance. The DGB is responsible for the policy integration between process domains. The CHoD is responsible for ensuring the integrality between process domains when designing processes in collaboration with HDFC for F&C processes. Control over the functioning of process domains or escalation of bottlenecks in the implementation occurs via the CHoD management consultations. Possible escalation occurs via the Readiness Consultation (RC) or the Defense Operations Consultation (DOC) and, finally, the Board Of Directors (BOD) as the highest Dutch military decision-making BOD. See Figure 28 for a schematic representation. [16]

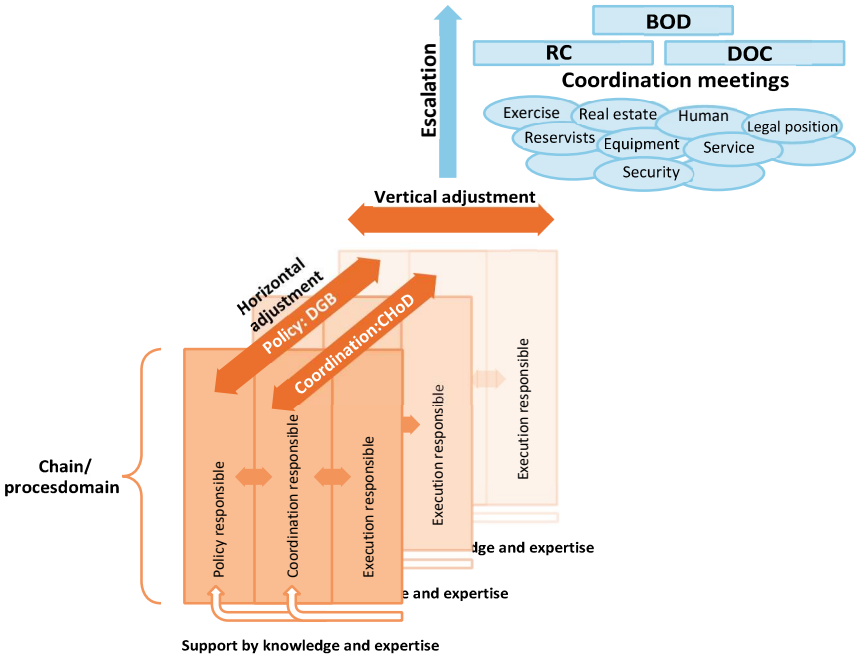


FIGURE 28 PROCESS MANAGEMENT [16]

APPENDIX J

Figure 29 describes the managed services for each layer, such as user-facing capabilities (e.g., end-user devices and applications) and back-end capabilities (e.g., middleware and networking) using the NATO NISP standard. [51]

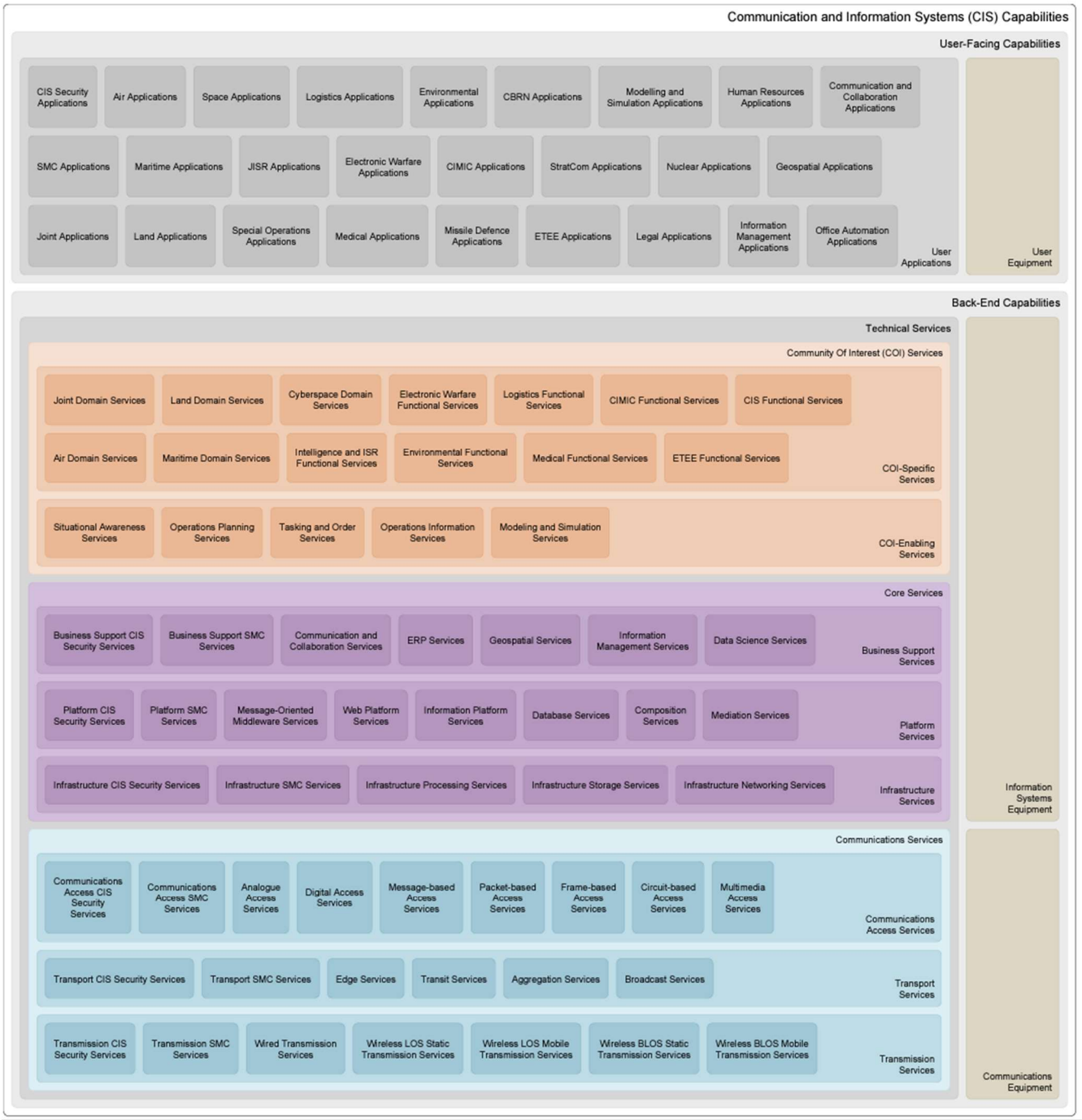


FIGURE 29 MANAGED SERVICES FOR EACH LAYER [51]

Depending on the chosen service model, the IT services are either internally managed (on-premise) or managed by an external (off-premise) IT service provider (see Figure 12: A, B, C, and D). From the perspective of the intra-cloud, interoperability is “the ability of two systems or clouds to exchange

and use information, to use each other's computing resources, to use each other software services, securely and seamlessly, while ensuring security and privacy." [52]

Interoperability in the cloud is actually a cloud of clouds only achievable if all cloud frameworks have a mechanism to interoperate. Therefore, it concerns the mutual sharing and use of information and each other's data, storage, processing, and IT services/software with the mutual consent of cloud owners and their users of IT services. [52] The level of mutual sharing between cloud owners and IT service users depends on the chosen software model. Figure 12 visualizes the sharing at infrastructure (dark purple), platform (light purple), or software (grey and orange) as a service level.

APPENDIX K

EECC: The EECC directive protects consumers whether they communicate through traditional (calls, SMS) or web-based services. It ensures all consumers can access affordable communications services, including broadband internet access for eGovernment, online banking, and video calls. [71]

ePrivacy: The European Commission adopted the proposal for the ePrivacy Regulation [96] in 2017 (replacing the current ePrivacy directive), in line with the General Data Protection Regulation (GDPR). While GDPR only applies to processing personal data, ePrivacy regulates electronic communication even if it concerns non-personal data. Also, in the case of cookies, the e-Privacy generally takes precedence. [63]

GDPR: The GDPR was created to support Article 8 of the European Charter of Human Rights [97] to protect personal data. In contrast, the ePrivacy regulation was designed to enshrine Article 7 of the charter concerning a person's private life, aimed to protect the confidentiality of communications, and put limits on tracking and spam. [62]
The GDPR aims to prevent and mitigate security breaches (Art. 32-1) and notify a supervisory authority of a breach of security that is likely to cause significant harm to services or individuals (Art. 33). To ensure consistent protection for natural persons throughout the union and prevent divergences hampering the free movement of personal data within the internal market. To demonstrate compliance with the GDPR, the controller[97] should adopt internal policies and implement measures that meet the principles of data protection by design and data protection by default. Such measures could consist, among other things, of minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency about the functions and processing of personal data, enabling the data subject to monitor the data processing, and enabling the controller to create and improve security features. As referred to in Article 30-1, the Data Protection Officer (DPO[98]) *"shall monitor compliance with this Regulation, with other Union or Member State data protection provisions, and with the policies of the controller or processor in relation to the protection of personal data."* [63] Each controller and, where applicable, the controller's representative shall maintain a record of processing activities under its responsibility as referred to in Article 30-1. The record shall contain information such as the purposes of the processing and a general description of the technical and, where possible, organizational security measures. Security measures as referred to in Article 32-1: "The controller and the processor[99] shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk" [63]. Article 32-1 describes a risk-based approach but does not define risk levels (or thresholds) as to what is appropriate.

NIS/NIS2: On 16 January 2023, Directive (EU) 2022/2555 (known as NIS2) [64] entered into force, replacing the NIS Directive (EU 2016/1148). [59] By October 17, 2024, EU member states must adopt and publish the NIS2 provisions[100] to legislation necessary to comply with the NIS2 directive. EU member states must identify the essential entities described in the NIS2 directive by April 17, 2025. [64] An important difference with the first NIS directive is that organizations automatically fall under the NIS2 directive if they are active in designated (see NCSC website) sectors, such as government services, and can be characterized as an "*essential*" or "*key*" entity. The services are essential for entities with more than 250 employees, such as the Dutch military. Essential entities are generally

[97] Controller: entity (party) that determines the why and the how for processing personal data (Article 4 GDPR).
[98] FG: Functionaris gegevensbescherming.
[99] Processor: entity (party) that performs the data processing on the controller's behalf (Article 4 GDPR).
[100] CER regulation (additional to NIS2): focuses on protecting public and private organizations against physical risks, such as the consequences of (terrorist) crimes, sabotage, and natural disasters. The European Commission adopted the CER regulation at the end of 2022. [98]

believed to have a much more disruptive impact on the economy and society than outages of *key* entities. The NIS2 directive contains a "*duty of care*" that obliges regulated entities to carry out a risk assessment by themselves, based on which they take appropriate measures to guarantee their services as much as possible and to protect the information used. The directive also requires entities to *"report incidents*" to the supervisor within 24 hours. These are incidents that (could) significantly disrupt the provision of essential services. In the event of a cyber incident, reporting to the Computer Security Incident Response Team (CSIRT) is required. Entities that fall under the NIS2 directive have a *"registration obligation."* Essential entities are subject to a more intensive "*supervision*" regime, namely ex-ante and ex-post supervision of compliance with the NIS2 directive, such as the *duty of care* and the commitment to *report incidents*. *Key* entities are 'only' accountable ex-post. The arrival of EU laws should contribute to more European harmonization and a higher level of cyber security in organizations. It is currently being worked out which sectors will fall under which supervisor (state-based agent). [98]

APPENDIX L

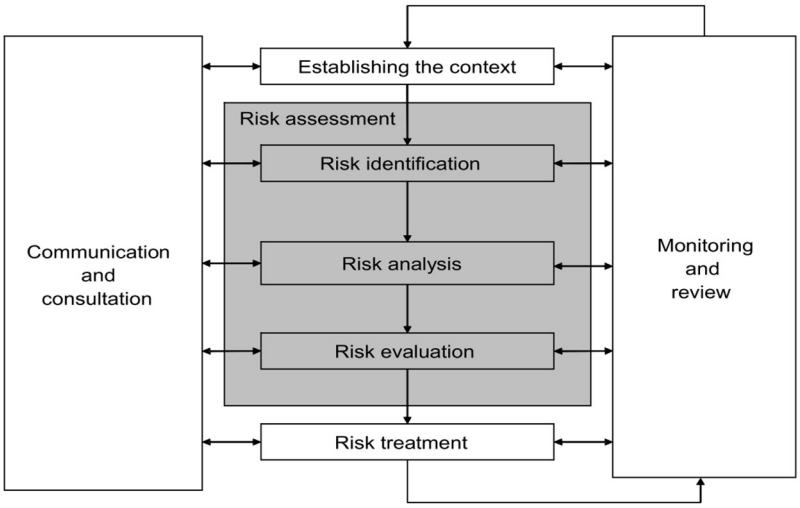


FIGURE 30 CONTRIBUTION OF RISK ASSESSMENT TO THE RISK MANAGEMENT PROCESS [82]

APPENDIX M

Examples of typical threat sources and threats are provided by the ISO standard 27005 Annex C [88] or below tables provided by the NIST standard 800-30 Rev1. [85]

Table 12 presents an overview of adversarial threat sources. [85]

TYPE OF THREAT SOURCE	THREAT DESCRIPTION
ADVERSARIAL - Individual (outsider, insider, trusted, privileged) - Group (ad-hoc or established) - Organization (competitor, provider, partner, customer) - Nation-state	Individuals, groups, organizations, or states seek to exploit society's dependence on cyber resources. - Social-engineering - System intrusion, break-ins, - Unauthorized system access - Browsing of personally identifiable information - Malicious code (e.g., virus) - System bugs - Identity theft - Spoofing
ADVERSARIAL - Standard user - Privileged user/Administrator	Individuals take erroneous actions in the course of executing everyday responsibilities.

TABLE 12 TYPES OF THREAT SOURCE (ADVERSARIAL) [85]

Table 13 shows examples of structural or environmental threat sources. [85]

TYPE OF THREAT SOURCE	THREAT DESCRIPTION
STRUCTURAL - IT Equipment (storage, processing, sensor, controller) - Environmental conditions • Temperature/humidity controls • Power supply - Software • Operating system • Networking • General-purpose IT service • Mission-specific IT service	Failures of equipment, environmental controls, or software; due to aging, resource depletion, or other circumstances which exceed expected operating parameters.
ENVIRONMENTAL - Natural or man-made (fire, flood, earthquake, etc.) - Infrastructure failure/outage (e.g. electrical)	Natural disasters and failures of critical infrastructures on which society depends but are beyond the organization's control, characterized by severity and duration.

TABLE 13 TYPES OF THREAT SOURCE (STRUCTURAL OR ENVIRONMENTAL) [85]

APPENDIX N

Table 14 and Table 15 are rating examples from the NIST "Risk Management Guide for Information Technology Systems."

Likelihood	Likelihood of threat occurrence definition
High	The threat source exists, is **highly** motivated, and sufficiently capable, or controls to prevent the vulnerability from being exercised are ineffective, or no controls are currently in place.
Medium	The threat source is motivated and capable, but controls are in place to impede the successful exercise of the vulnerability.
Low	The threat source exists but **lacks** motivation or capability, or controls are in place to prevent or significantly impede the vulnerability from being exercised.

TABLE 14 LIKELIHOOD OF OCCURRENCE RATING [86]

Ease of exploitation rating	Ease of exploitation of a vulnerability definition
High	**Easy** exploitation of the vulnerability.
Medium	**Some** knowledge and/or tools are required to exploit the vulnerability.
Low	**Extensive** knowledge and/or tools are required to exploit the vulnerability.

TABLE 15 EASE OF EXPLOITATION RATING [86]

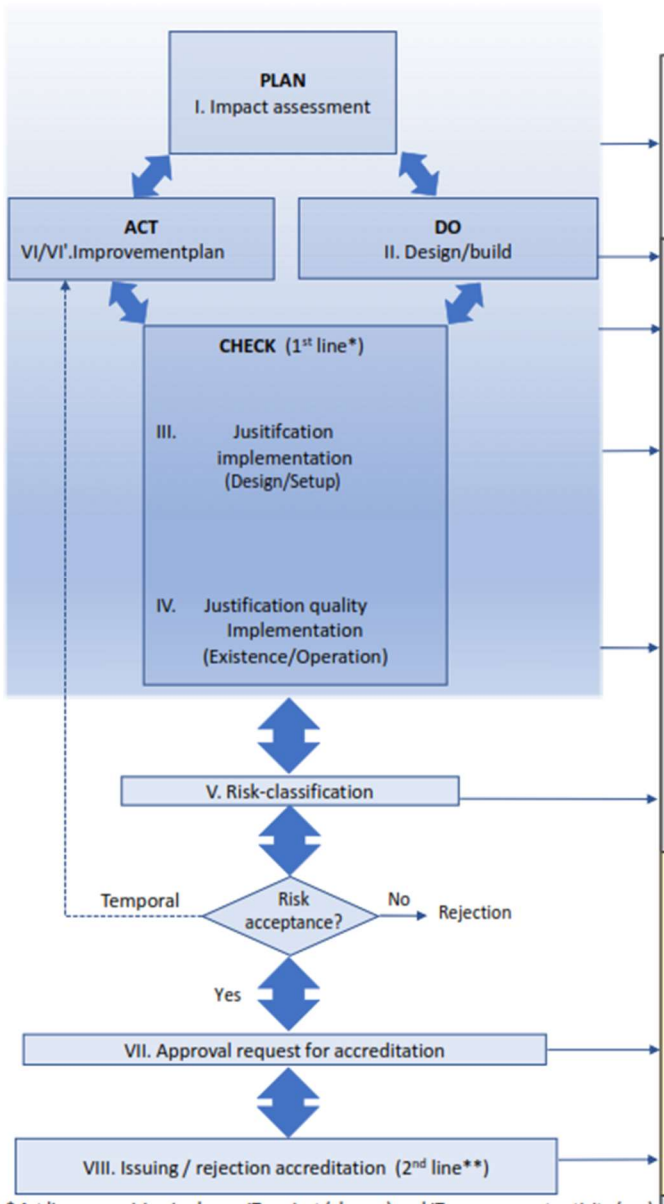
APPENDIX O

Table **16** presents an example from the NIST "Standards for Security Categorization of Federal Information and Information Systems" (FIPS PUB 199). [99]

	Potential impact (consequence)		
Security Objective	**Low**	**Medium**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have **a severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

TABLE 16 POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES [99]

APPENDIX P



	#	Information exchange (Documentation)	Approval
PLAN	I	a. Security Impact Assessment b. Privacy Impact Assessement c.Agreement on used frameworks consisting of best practice norms or controls relevant for the COI involved (Jurisdiction) **d. Agreement with Supervisor (2nd line**) on approach for system / sample check**	Mandatory
DO	II	a. PSA/Technical design (Change/Run) b. Vulnerability assessment	Madatory
	III	Jusitification implemented security measures (design/setup): a. Interview based (all norms) b. Documented (all norms) c. Focus areas or themes *** (selected norms) d. Integral systemdescription (1 document)	Comply/ explain
	IV	Jusitification implemented security measures (existence/operation): a. Security acceptance test report b. Audit report c. NBV report d. Security assessment report (e.g. Pentest) e. Inspection report (on location)	Comply/ explain
	V	Final risk classification (heatmap)	Madatory
CHECK	VI	Risk acceptance/handling by owner: a. Statement of Compliance (IT system / Interface) b. ACT phase --> **intervention**: improvment plan for mitigating temperal risks (1th line assurance budget, resources, planning etc)	Mandatory
	VII	Request for accreditation / approval for use	Mandatory
	VIII	a. Approval to Operate (TBB1/TBB2/Critical) b. Certification interfaces c. Assessments operation phase (All MOD IT)	Mandatory
ACT	VI'	a. Dynamic trigger for ACT step: **Incident** due to known/unknown threats or vulnerabilities --> **Short term intervention** --> Incident / crisis handling / short term improvement plan b. trigger for ACT step: changed or new functionality, known threats or vulnerabilities or experid approval (3 years) --> **Intervention** --> Start with PLAN phase	Comply/ explain

* 1st line supervision is also an IT project (change) and IT management activity (run) requiring imely allocation of budget, resources, expertise, etc.
** 2nd line supervision is a MOD Security Authoririty or Sectorial supervisory body activity. The Security Authority is supported by 1st line security coordinators and security officers on (MOD) unit level.
*** Example themes: patch or autorization management, logging & monitoring, segmentation, identify, protect, detect, respond, recover etc.
Note: The 1st line supervisor in support of change and run (as mentioned above) checks all security aspects. The 2nd line supervisor (supported by 1st line security coordinators) execute sample / system (operation PDCA cycle) checks on security as agreed on in step I-d.

FIGURE 31 EIGHT-STEP PLAN FOR OBTAINING APPROVAL FOR USING IT PLATFORM SERVICES