The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act

Final Report

Irene Kamara, Ronald Leenes, Kees Stuurman, Jasper van den Boom

Tilburg Institute for Law, Technology, and Society

This study is commissioned by the National Cyber Security Centre of the Netherlands

July 2020

Report title	**The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act**
Authors	Irene Kamara, Ronald Leenes, Kees Stuurman, Jasper van den Boom
Affiliation	Tilburg Institute for Law, Technology, and Society Department of Law, Technology, Markets, and Society Tilburg Law School
Version	Final Report
Date	30 July 2020
Funding	Nationaal Cyber Security Centrum (NCSC)

The authors would like to thank Philippe Martens and Bilgesu Sumer for their research assistance.

Abbreviations

ACM	Dutch Authority for Consumers & Markets
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
Bbni	Besluit Beveiliging Netwerk- en Informatiesystemen
CAB	Conformity Assessment Body
COVA	Stichting Centraal Orgaan Voorraadvorming Aardolieproducten
CSA	Cybersecurity Act
CSCT	Cross Sector Cyber Test Bed
CSIRT	Computer Security Incident Response Team
DSO	Distribution System Operator
GDPR	General Data Protection Regulation (EU) 679/2016
EAL	Evaluation Assurance Level
ENCS	European Network for Cyber Security
ENTSO-E	European Network of Transmission System Operators for Electricity
ENTSO-G	European Network of Transmission System Operators for Gas
ETSI	European Telecommunications Standards Institute
EU-CC	EU Common Criteria scheme
ISAC	Information Sharing and Analysis Centre
ISO	International Organisation for Standardisation
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
MRA	Mutual Recognition Agreement
MS	EU Member State
NAB	National Accreditation Body
NAM	Nederlandse Aardolie Maatschappij
NBV	Nationaal Bureau voor Verbindingsbeveiliging
NCCA	National Cybersecurity Certification Authority
NCSA	Nationale Cybersecurity Agenda
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NDA	Nationale Distributie Autoriteit
NEN	Dutch Standardisation Organisation
NESAS	Network Equipment Security Assurance Scheme
NIS	Network and Information Security
NIST	US National Institute for Standards and Technology

NSCIB	Nederlandse Schema voor Certificatie op het gebied van IT-Beveiliging
OES	Operator of Essential Services
OvJ	District Attorney (Officier van Justitie)
PSD2	Payment Services Directive (EU) 2015/2366
RvA	National Accreditation Body
SCADA	Supervisory Control and Data Acquisition
SDO	Standard Development Organisation
SME	Small Medium Enterprise
SOG-IS	Senior Officials Group Information Systems Security
Sw	Sanctiewet 1977
TSO	Transmission System Operator
UAVG	Implementing Law of the General Data Protection Regulation
Wbni	Wet Beveiliging Netwerk- en Informatiesystemen
Wft	Wet op het financieel toezicht
Wgmc	Wet Gegevensverwerking en Meldplicht
Wiv 2017	Wet op de Inlichtingen en Veiligheidsdiensten 2017
Wtt	Wet toezicht trustkantoren
Wvsr	Wetboek van Strafrecht
Wwft	Wet ter voorkoming van witwassen en financieren van terrorisme

Table of Contents

Executive summary

- The Netherlands is one of the most digitalised countries worldwide. However, digitalisation comes with vulnerabilities, as demonstrated with incidents such as the NotPetya case in 2017 and the 2019 Maastricht University incident. There are several ways to address such cybersecurity issues, standards and certifications are one of them. Especially certification as an instrument of regulation is rising after the 2019 Union Cybersecurity Act, which introduced a framework for European cybersecurity certifications.
- Against this background, the research aimed at sketching the cybersecurity certification landscape in the Netherlands, identify the impact of the Union Cybersecurity Act (CSA) on stakeholders such as industry and conformity assessment bodies, and make an inventory of potential roles for the NCSC in this setting.
- The main instruments of the EU legislation on cybersecurity are the NIS Directive and the CSA, while there are more laws which touch upon cybersecurity, including information security, matters such as the Radio Equipment Directive.
- The Dutch legal framework on Cybersecurity is mainly the Network and Information Systems Security Act (Wbni), which is the implementation of the NIS Directive, and organisational decrees and Ministerial Decisions. The adaptation law of the Union Cybersecurity Act has not been published yet. It is expected to designate the Ministry of Economic Affairs and Climate, and its Radiotelecommunications Agency, as the national cybersecurity certification authority.
- The Netherlands follows a decentralised model, whereby several agencies and Ministries have competences in cybersecurity. The NCSC in the Netherlands is part of the Ministry of Justice and Security and its tasks are mainly stemming from the NIS Directive and its implementing legislation (Single Point of Contact, CSIRT, support to Operators of Essential Services, technical analysis and research, information dissemination and others). Other actors include the Radiotelecommunications Agency, the General Intelligence and Security Service, the National Bureau for Security Connections, the Military Intelligence and Security Service, and the Digital Trust Centre.
- Public Private Partnerships have a substantial role in cybersecurity in the Netherlands. The Information Sharing and Analysis Centres (ISAC), which are sectoral network initiatives, developed and operating under the lead of the NCSC, are an example. Other examples include: Partnering Trust, the Dutch Secure Software Alliance and Zeker-Online.
- In analysing the conformity assessment part of the Dutch cybersecurity certification landscape, it is evident that in the Netherlands there are both national but also many conformity assessment bodies operating internationally. These multinational activities influence the positioning of CABs, which do not follow only local developments and have an interest to strengthen their governmental relations not only within the Netherlands, but also cross-border. According to interviewed CABs, trust, reliability, reputation with partners and consumers, and first-movers advantage are drivers for cybersecurity certification. The most important driver is legislation and certification being mandatory. Costs are reported as obstacles, and for this reason some CABs offer alternatives such as assessment based on non-formal standards.
- The research on the views of the industry (energy and banking sector) showed that while companies are interested/ or sometimes obliged to conform to cybersecurity standards, they are not always motivated to pursue certification. Stringent documentation requirements and high costs are obstacles for certification. Mandatory certification is deemed desirable by some energy OES in the Netherlands, while this is not the case in the banking sector, as the multitude of standards and specifications already imposed on the sector requires extensive resources for compliance. Improvement of internal security, trust with consumers, demonstrating compliance with legal obligations to the regulator, and cross-border cooperation are some of the drivers for certification, while awareness for its added value is viewed as necessary.

- When it comes to state of the art and new developments in standardisation and certification, the research showed that formal standards are a preferred option for certification. Cross-sector standards such as the ISO/IEC 27001, the Common Criteria, the IEC 62443 for Industrial Automation and Control Systems are preferred solutions. Further, cryptography standards, the NIST Cybersecurity Framework and some informal standards are used as reference documents. Several sector specific standards are also used, such as the ETSI 303 645 on IoT.
- With regard to the (expected) impact of the CSA on the Dutch cybersecurity certification stakeholders, some CABs reported new business opportunities and re-arrangement of the market, while some others showed hesitation and doubts about the market demand. The energy and banking sectors, view the CSA as stimulating the market, but do not expect a direct impact, since certifications are (still) voluntary. However, European certifications in relevant areas, such as IoT and cloud, are expected to have an indirect impact on energy companies and banks.
- Last, an inventory of potential roles for the NCSC was drafted, based on the analysis of the Dutch legal framework, the opportunities created by the CSA, and the needs, drivers, obstacles reported by the Dutch cybersecurity certification stakeholders. Those options were explored as a thought provoking exercise for further outlook and discussion, and do not delve into matters of internal capacity and resources or feasibility in view of the relations with other governmental agencies.
- Those potential roles range from supportive, reactive to proactive ones. Facilitating knowledge sharing on cybersecurity certifications via national ISACs, or other informal collaborations, raising awareness and conducting trainings, expanding voluntary collaborations with certification bodies and other stakeholders are in general roles within the current mandate of the NCSC, with strong supportive role. The NCSC could also explore the option of providing substantial assistance to the national cybersecurity certification authority in providing advice during the assessments of high assurance certifications, or providing aggregated data on deficiencies in the implementation of schemes. Alternatively, the NCSC could lend its expertise to the National Accreditation Body when conducting assessments of certification bodies. Further, continuing and systematizing the current work of the NCSC in standardisation, could be valued by its partners, as promoting their interests at national, European, and international fora. Last, following the example of the National Cyber Security Centers of other countries, the NCSC-NL could develop its own national scheme and label, in areas not covered by the European cybersecurity certifications.
- All those options, bring forward two main elements of the NCSC: the trusted partnerships and deep expert knowledge in the field. The study showed that there are issues to be considered when adopting those options such as expanding its legal mandate. On top of any future role of the NCSC in the certification landscape in the Netherlands, the NCSC should keep an eye for other forthcoming related developments, which may strengthen its mandate, such as the ongoing revision of the NIS Directive.

Samenvatting

- Nederland is een van de meest gedigitaliseerde landen ter wereld. Digitalisering gaat echter gepaard met kwetsbaarheden, zoals de NotPetya-zaak in 2017 en het incident van de Universiteit Maastricht in 2019. Er zijn verschillende manieren om dergelijke cyberbeveiligingsproblemen aan te pakken. Bijvoorbeeld met het gebruik van normen en certificeringen. Vooral het gebruik van certificering als reguleringsinstrument neemt toe na de Union Cybersecurity Act 2019 waarmee een regelgevend kader wordt geïntroduceerd voor Europese cyberbeveiligingscertificeringen.
- Tegen deze achtergrond is het onderzoek gericht op het schetsen van het landschap van cyberbeveiligingscertificering in Nederland, het identificeren van de impact van de Union Cybersecurity Act (CSA) op belanghebbenden zoals de industrie en conformiteitsbeoordelingsinstanties, en het inventariseren van mogelijke rollen voor het NCSC binnen dit landschap.
- De belangrijkste instrumenten van de EU-wetgeving inzake cyberbeveiliging zijn de NIS-richtlijn en de CSA, maar er zijn ook andere wetten die betrekking hebben op cyberbeveiliging en informatiebeveiliging, zoals de radioapparatuur richtlijn.
- Het Nederlandse rechtskader voor cyberveiligheid bestaat voornamelijk uit de wet op de beveiliging van netwerk- en informatiesystemen (Wbni), organisatorische besluiten en ministeriële besluiten. De aanpassingswet van de Union Cybersecurity Act is nog niet gepubliceerd. Het wordt verwacht dat in de aanpassingswet het Ministerie van Economische Zaken en Klimaat, en het daaronder vallende Bureau voor Radiotelecommunicatie, wordt aangewezen als de nationale certificeringsinstantie voor cyberbeveiliging.
- Nederland volgt een gedecentraliseerd model, waarbij verschillende instanties en ministeries bevoegdheden hebben op het gebied van cybersecurity. Het NCSC in Nederland maakt deel uit van het ministerie van Justitie en Veiligheid en haar taken vloeien voornamelijk voort uit de NIS-richtlijn en de Wbni (Single Point of Contact, CSIRT, ondersteuning aan exploitanten van essentiële diensten, technische analyse en onderzoek, informatieverspreiding) en anderen). Andere actoren zijn onder meer Agentschap Telecom, de Algemene Inlichtingen- en Veiligheidsdienst, het Nationaal Bureau voor Verbindingsbeveiliging, de Militaire Inlichtingen- en Veiligheidsdienst en het Digital Trust Center.
- Publiek-private samenwerking speelt een substantiële rol in het Nederlandse landschap inzake cybersecuritycertificering. Een voorbeeld hiervan zijn de informatie-uitwisselings- en analysecentra (ISAC). Dit zijn sectorale netwerkinitiatieven die functioneren en ontwikkeld worden onder leiding van het NCSC. Andere voorbeelden zijn: Partnering Trust, de Dutch Secure Software Alliance en Zeker-Online.
- Bij het analyseren van het conformiteitsbeoordelingsgedeelte van het Nederlandse cyberbeveiligingscertificatielandschap is het duidelijk dat er in Nederland conformiteitsbeoordelingsinstanties zijn die zowel nationaal en internationaal actief zijn. Deze multinationale activiteiten beïnvloeden de positionering van CBI's aangezien zijn niet alleen lokale ontwikkelingen volgen maar er ook belang bij hebben hun bestuurlijke relaties op grensoverschrijdend vlak te versterken. Volgens geïnterviewde CIB's zijn vertrouwen, betrouwbaarheid, reputatie bij partners en consumenten, en het first-moversvoordeel drijfveren voor cyberbeveiligingscertificering. De belangrijkste drijfveren zijn echter wetgeving en het verplicht stellen van certificering. De kosten die gepaard gaan met certificering worden gerapporteerd als een obstakel en daarom bieden sommige CBI's alternatieven aan, zoals beoordeling op basis van niet-formele normen.
- Uit het onderzoek naar de opvattingen van de industrie (energie- en banksector) bleek dat bedrijven weliswaar geïnteresseerd en soms verplicht zijn om te voldoen aan cyberbeveiligingsnormen, maar niet altijd gemotiveerd zijn om certificering na te streven. Strenge documentatievereisten en hoge kosten zijn belemmeringen voor certificering. Verplichte certificering wordt door sommige energie-OES in Nederland wenselijk geacht, terwijl dit in de banksector niet het geval is vanwege het veelvoud aan

normen en specificaties die al aan de sector zijn opgelegd en de daaraan verbonden nalevingskosten. Verbetering van de interne veiligheid, vertrouwen bij de consument, het aantonen van compliance aan de wetgever en grensoverschrijdende samenwerking zijn enkele drijfveren voor certificering. Bewustzijn voor de toegevoegde waarde van certificering wordt tevens noodzakelijk geacht.

- Als het gaat om state-of-the-art en nieuwe ontwikkelingen op het gebied van standaardisatie en certificering, toonde het onderzoek aan dat formele standaarden een voorkeursoptie zijn voor certificering. Sectoroverschrijdende standaarden zoals de ISO/ IEC 27001, de Common Criteria, de IEC 62443 voor industriële automatisering en controlesystemen zijn voorkeursoplossingen. Verder worden cryptografische standaarden, het NIST Cybersecurity Framework en enkele informele standaarden gebruikt als referentiedocumenten. Er worden ook verschillende sectorspecifieke normen gebruikt, zoals de ETSI 303 645 voor IoT.
- Met betrekking tot de (verwachte) impact van de CSA voor Nederlandse stakeholders, meldden sommige CBI's nieuwe zakelijke kansen en een nieuwe marktordening, terwijl anderen hun twijfels hadden bij de marktvraag voor certificering. De energie- en banksector zien de CSA als stimulerend voor de markt, maar verwachten geen directe impact, aangezien certificeringen (nog) vrijwillig zijn. Europese certificeringen op relevante gebieden, zoals IoT en cloud, zullen naar verwachting een indirecte impact hebben op energiebedrijven en banken.
- Ten slotte is een inventarisatie gemaakt van mogelijke rollen voor het NCSC op basis van de analyse van het Nederlandse wettelijke kader, de kansen die de CSA heeft gecreëerd en de behoeften, drijfveren, belemmeringen die door de Nederlandse cybersecurity-certificeringsactoren zijn gemeld. Deze inventarisatie is gemaakt als een tot nadenken stemmende oefening voor verder vooruitzicht en discussie, en gaan niet in op kwesties van interne capaciteit en middelen of haalbaarheid in het licht van de relaties met andere overheidsinstanties.
- De potentiële rollen variëren van ondersteunend, reactief tot proactief. Het faciliteren van het delen van kennis over cyberbeveiligingscertificeringen via nationale ISAC's of andere informele samenwerkingen, het vergroten van het bewustzijn en het geven van trainingen, het uitbreiden van vrijwillige samenwerkingen met certificeringsinstanties en andere stakeholders vallen in het algemeen binnen het huidige mandaat van de NCSC waarbij de nadruk ligt op een ondersteunende rol. Het NCSC zou ook de mogelijkheid kunnen onderzoeken om de nationale cyberbeveiligingscertificeringsautoriteit aanzienlijke bijstand te verlenen door advies te verstrekken bij de beoordeling van 'high assurance' certificeringen, of om geaggregeerde gegevens te verstrekken over tekortkomingen bij de uitvoering van regelingen. Als alternatief zou het NCSC zijn expertise kunnen uitlenen aan de nationale accreditatie-instantie bij het uitvoeren van beoordelingen van certificatie-instellingen. Verder zou de voortzetting en systematisering van het huidige werk van de NCSC op het gebied van standaardisatie door haar partners kunnen worden gewaardeerd aangezien NCSC hun belangen zou kunnen behartigen op nationale, Europese en internationale fora. Ten slotte zou NCSC-NL, naar het voorbeeld van de nationale cyberbeveiligingscentra van andere landen, een eigen nationaal schema en label kunnen ontwikkelen op gebieden die niet onder de Europese cyberbeveiligingscertificeringen vallen.
- Al deze opties brengen twee hoofdelementen van het NCSC naar voren: de vertrouwde partnerschappen en diepgaande vakkennis in het veld. Uit de studie bleek dat er bij de vaststelling van de verscheidene opties rekening moet worden gehouden met een mogelijke uitbreiding van het wettelijke mandaat. Naast elke toekomstige rol van de NCSC in het certificeringslandschap in Nederland, moet het NCSC ook oog hebben voor andere aanstaande gerelateerde ontwikkelingen, die haar mandaat kunnen versterken, zoals de voortdurende herziening van de NIS-richtlijn.

1 Introduction

1.1 Background and aims of the Report

The Netherlands is one of the most digitalised countries worldwide.[1] However, digitalisation comes with vulnerabilities, as demonstrated with incidents such as the NotPetya case in 2017[2] and the increasing supply chain compromise in software and through cloud objects.[3] Despite the investments in cybersecurity, there are new vulnerabilities and new targets, such as educational institutions,[4] and new threats which render cybersecurity and the assessment of the level of a company's cybersecurity an ongoing concern for organisations. Cyberattacks or compromises in the overall security of products or systems may have potential adverse impacts on governmental functionalities, businesses, individual users, the society at large and national security. A recent example is a data breach in the "RIVM infection radar" which may have resulted in disclosure of sensitive health information, who participated in the Infection Radar.[5]

Research and practice have shown that standardisation and conformity assessment are valuable tools in enhancing cybersecurity, and addressing issues unlikely to be resolved by a single company or organisation. Standards codify and accumulate the knowledge and best practices of significant players in the cybersecurity field. Accordingly, certification by accredited conformity assessment bodies offers the potential of an independent audit by a third party (the CAB) and the reliable attestation for the level of security of an organisation's processes, products, systems, or services.

There is a variety of standards development organisations (SDOs) working on cybersecurity standards. Formal standardisation bodies, such as the NEN in the Netherlands, CEN, CENELEC and ETSI at EU level, and ISO, IEC, and ITU at international level, are working in parallel to a variety of informal organisations and industry fora and consortia such as OASIS, OWASP, W3C, IETF and others.[6] Standards and certification schemes based on those standards are developed for different aspects of the security lifecycle of "Assess - Design – Manage – Monitor - Deploy", such as:[7]

- Security feature provision
- Security assurance
- Security threat sharing
- Organisational management for secure operations.

In addition, standards in the broader cybersecurity field are often classified as ICT related security standards, cybersecurity standards, risk management standards (such as the NIST Special Publication 800-30 providing guidance for conducting risk assessments) and others.[8]

At the same time, certification as an instrument of regulation is rising. In 2019, the Cybersecurity Act introduced a framework for European cybersecurity certifications. The European Cybersecurity Certification Framework is expected to provide a baseline mechanism for further development of cybersecurity certification schemes at EU level with the aim to attest that ICT products, ICT services, ICT processes "comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle." The Cybersecurity Act adopts a centralised model, whereby the European Commission and ENISA play a pivotal role in developing and adopting cybersecurity certification schemes, leading to a more harmonised landscape. In the implementation phase, national actors in the Member

States take over the assessments, granting of certifications, and being responsible for supervision. National authorities of the Member States need to re-assess how they position themselves in the new landscape and identify areas to improve and update their role both at national and EU level.

Following these developments, the Nationaal Cyber Security Centrum (NCSC) identified a strategic need for an insight in the Dutch certification landscape, the upcoming changes due to the EU developments, as well as an exploration of the potential (supporting) roles of the NCSC. Against this background, the research aimed at sketching the cybersecurity certification landscape in the Netherlands, identify the impact of the Union Cybersecurity Act so far on stakeholders such as the industry and conformity assessment bodies, and make an inventory of potential roles for the NCSC in this setting.

1.2 Cybersecurity and certification: working definitions

Cybersecurity is a broad concept, for which multiple definitions exist. The US National Institute for Standards and Technology (NIST) defines cybersecurity as "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."[9] Other definitions focus on the type of activities to be undertaken by an organisation,[10] or the goal of protection of systems, or of property rights.[11]

As the High Level Group of Scientific Advisors of the European Commission has explained, cybersecurity as an academic field of study combines a multiplicity of disciplines, ranging from technical to cultural behavior.[12] Indeed, a grammatical or hermeneutical approach in defining cybersecurity might lead to different results on how the term is used in practice and legislation.[13]

Focusing on the Union legislation, the recently adopted EU Cybersecurity Act defines cybersecurity as:

> *"the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber-threats."*[14]

The definition includes two types of targets that are deemed to need protection: systems and persons. Network and information systems, according to the NIS Directive include an electronic communications network,[15] any device or interconnected or related devices, "one or more of which, pursuant to a program, perform automatic processing of digital data", or "digital data stored, processed, retrieved or transmitted" for the purposes of their "operation, use, protection and maintenance".

The protection of a network and information security system[16] relates to the ability of network and information systems to resist actions that compromise the availability, authenticity, integrity or confidentiality of data.[17] At the same time, cybersecurity does not deal only with technology, but also with human behavior.[18] Cyberthreats are directed and affect anything that can damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons. The CSA definition includes also another category of individuals: those that while are not using the given system, are nonetheless affected by cyberthreats. This category expands the scope of cybersecurity significantly, as anyone can potentially be affected by cyberthreats. Thus, individuals are part of the problem, as potential threats, but also a protected group, as targets. Important for an understanding of the scope of cybersecurity is to note that, according to ENISA, network and information security are subsets of cybersecurity.[19] In this study, we adopt the cybersecurity definition as provided in the EU

Cybersecurity Act, since the scope of the study relates closely to the developments and impact of the EU CSA in the Netherlands.

Related to the broad scope of what falls under the definition of cybersecurity is the issue of which aspects, domains, and sectors pertain to cybersecurity. The taxonomy by the Joint Research Centre is the starting point and guiding document for our research.[20] The holistic taxonomy is constituted by three dimensions:

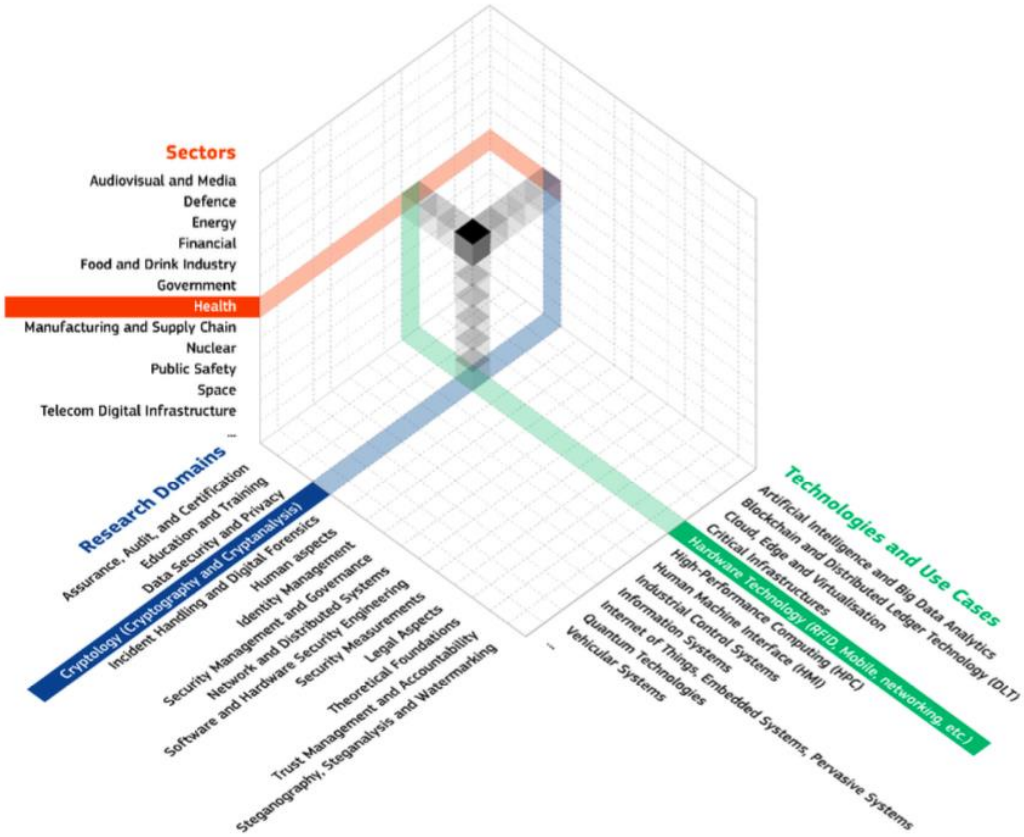


Figure 1: JRC High-level holistic cybersecurity taxonomy

- **Cybersecurity domains**, which represent areas of knowledge in relation to different aspects of cybersecurity.
- **Sectorial Dimensions**, which help contextualise cybersecurity, requirements and challenges in different sectors e.g. energy.
- **Technologies and use case dimensions**, which represent technological aspects of the cybersecurity domains.

The JRC taxonomy gives an overview of the landscape and the different dimensions of cybersecurity. For the selection of relevant sectors at large for the study, we navigated through the JRC taxonomy with the priority sectors of the Network and Information Security Directive as drivers.[21] Those sectors and subsectors for the two types of regulated entities (Operators of Essential Services and Digital Service Providers) are:[22]

OES Sectors NIS Directive	Subsector
Energy	Electricity, oil, gas.

Transport	Air transport, rail transport, water transport, road transport.
Banking	N/A
Financial market and infrastructures	N/A
Health sector	Healthcare settings
Drinking water supply and distribution	N/A
Digital Infrastructure	
Digital Service Providers NIS Directive	
Online marketplace	
Online search engine	
Cloud computing service	

Table 1: NIS Directive regulated sectors

The scope of the research of this study required focusing mainly on the dimension of sectors, as a means to provide insights for cross-sector use, and the research domain (certification). The research kept an open eye for the third dimension of the taxonomy (technology).

When it comes to defining certification, there are several well-accepted definitions. The ISO/IEC 17000 standard providing definitions of conformity assessment terms, defines certification as: "third-party attestation, related to an object of conformity assessment," that is an object such as product, service, system, data, design, body etc., to which specified requirements apply. [23] Significant element of the definition is that a third party is conducting the assessment and grants the certification. This provides guarantees of an independent assessment, and essentially makes certification a trust mechanism. Further, when the conformity assessment body – certification body, lab, inspection body – is itself going through an assessment of its independence, integrity, capacity and competence, we speak of accreditation. Certification is conducted on the basis of a certification scheme, which as the Union Cybersecurity Act provides, it is a "comprehensive set of rules, technical requirements, standards, and procedures".[24]

1.3 Identification of stakeholders

The consultation of stakeholders is essential to help define the role of NCSC in cybersecurity certification. Cybersecurity (certification) likely plays a different role for different stakeholders and if NCSC is to advise stakeholders it is important to understand their take on cybersecurity (certification). This section describes how we made a selection of the types of organisations that are considered as 'stakeholders' for the project. Being a stakeholder means that the views/needs or practices of a given type of organisation are important to be collected and considered in order to reach a set of Recommendations.

The stakeholder identification was based on the analysis of the relevant legislation such as the Cybersecurity Act, the NIS Directive, the Wbni, the developments at EU level on cybersecurity certification (e.g. *ad hoc* working groups), and existing studies. We focused on the national dimension, but keeping an eye on EU developments that may shape cybersecurity policy further down the line.

For gathering the input of the stakeholders, the approach was to be inclusive, instead of *prima facie* selectiveness, taking into account however practical constraints of the project such as time, budget, and availability or interest of the stakeholders. The outcome of the above exercise is the list of stakeholder groups outlined in this section of the Report. It should be noted that the goal of the exercise is not representation of any possible group, but a sufficient coverage of needs and interests, and expertise or knowledge on the research questions of the project.

1.3.1 Standardisation Body and National Accreditation Body

The Dutch Standardisation Organisation (NEN) is active in developing national standards in the field of information security and cybersecurity. Standardisation experts in the ICT standardisation cluster at NEN are relevant for the project as they stir and impact the certification landscape to a certain extent. In addition, NEN also participates in the European Standardisation Organisations' Technical Committees active in the field such as the Joint Technical Committee CEN/CLC/JTC 13 Cybersecurity and Data Protection, as well as the international standardisation organisations, such as ISO and IEC.[25]

The National Accreditation Council (Raad voor Accreditatie) plays quite an important role in the landscape, especially since the Cybersecurity Act establishes mandatory accreditation for certification bodies that intend to offer services on the European cybersecurity certification schemes. The National Accreditation Body will provide accreditation in line with the CSA schemes.

Beyond the formal standardisation organisations recognized by Union legislation, there are initiatives and platforms in the field of standardisation. One example is the Standardisation Forum (Forum Standaardisatie), which aims to promote interoperability and supplier independence through the use of open standards for digital data exchange in the public sector. The Forum consists of experts from various government organizations, business and science.[26] Part of the thematic portfolio of the Standardisation Forum concerns the Internet and security related standards.[27] Another example is the Platform for Internet Standards (Platform Internetstandaarden), which promotes specifications for safe digital processes and infrastructure in a number of domains such as health, privacy, Artificial Intelligence, and Internet Governance.[28]

1.3.2 Industry vendors and users

The consultation of industry is essential to identify what are the future topics and domains of certification that the industry in the Netherlands would expect developments, and how the NCSC could play a role in supporting those needs and developments. Priority and the main focus is on the industry stakeholders established in the Netherlands, including producers, service providers, (vendors) and users, procurers. To some limited extent, representatives of industry at EU level are also considered stakeholders for this study. An example is the European Cybersecurity Organisation (ECSO), which is the European Commission's counterpart on contractual Public-Private Partnerships (cPPPs).[29]

1.3.3 Conformity Assessment Bodies

Another stakeholder group is that of the conformity assessment bodies conducting tests and performing evaluations for cybersecurity certification in the Netherlands. The research focuses on accredited certification bodies, due to the high quality guarantees those bodies offer, as prescribed by the relevant EU legislation.[30]

1.3.4 Government and Regulators

The cybersecurity regulatory landscape in the Netherlands is complex, as outlined in Chapter 2. The CSA and the introduction of new powers for authorities on cybersecurity certification, and the goals of the study require that those governmental actors competent in the field of cybersecurity are consulted.

1.3.5 Civil Rights associations and academia

While not directly involved in cybersecurity certification, this group of stakeholders shows the impact of the lack of cybersecurity certification or of a bad quality certification, to the individual due to the potential or concluded cyberattacks.

1.4 Methodology and Structure of the Report

The research for this Report followed a mix of methods, which include doctrinal legal analysis (Chapters 2 and 3), literature review and analysis of policy and technical documentation (standards and certification schemes) (Chapters 2-7), stakeholder analysis (Chapters 4-7) and semi-structured interviews with experts (Chapters 4-7). The combination of methods offered a balanced approach in addressing the project aims. The literature review provided first insights on cybersecurity certifications in the Netherlands, alongside conformity assessment bodies, such as certification bodies and laboratories. Further, the analysis of the legal framework in which the NCSC operates, but also of the new EU legal framework affecting the national landscape set an essential basis for the further research of the project. The stakeholder identification and analysis, together with semi-structured interviews with selected experts, informed and refined the initial findings and contributed to comprehensive outlook for potential roles.

With regard to the empirical research of this project, the research team interviewed 26 experts in May and June 2020. The aim of the semi-structured interviews was to obtain information related to the main goals of the study as stated above, and to test the findings from the literature review and the legal analysis. The selection criteria for the conformity assessment bodies included establishment of HQ or operational office in the Netherlands, experience in the field of cybersecurity certification, accreditation from the Dutch Accreditation Council (Raad voor Accreditatie), which is a formal requirement imposed by the EU Cybersecurity Act. Interview requests have also been sent to a limited number of companies from the energy sector and the finance sector, in coordination with the NCSC. The expert selection of the governmental contacts was facilitated by the NCSC. The interviews were conducted via videoconferencing, in Dutch and in English. The findings were validated and enriched in a feedback workshop with invited experts from the National Cyber Security Centre.

Regarding the scope and limitations of the research: The Report aims at bringing insights that can be applied cross-sector. The EU Cybersecurity Act, which triggered the interest for this Report, is not a sectorial law and hence exploring different sectors may bring different insights in the needs of the various stakeholders. This approach is justified also from standardisation in the field and certification, which adopt a cross-sector approach when it comes to baseline requirements, and often relate to sectors for fine-tuning the requirements or adding layers on top of the basic requirements. This is why in the stakeholder identification, we are interested in regulators, standardisation and certification actors with an expertise in cybersecurity (certification), not focusing on specific sectors. Nonetheless, there are two issues which demand a different approach when it comes to industry (vendors and consumers/users) stakeholders. One is that inevitably, due to the limited mandate for this

project, a full scale empirical research covering all the different relevant sectors was impossible due to resource limitations. Second, the mandate of the NCSC plays an important role. If our aim is to provide useful recommendations for potential (advisory) roles of the NCSC in the field of cybersecurity certification in the Netherlands, the entities connected from a regulatory perspective to the NCSC (Partners en doelgroepen) should be the main focus of the research. Since the NCSC is the Single Contact Point and the Computer Security Incident Response Team (CSIRT) in line with the Network and Information Security Directive (NIS) and its national implementation in the Netherlands (Wbni), the Operators of Essential Services and the Digital Service Providers were the possible candidates. From the OES (vitale aanbieders) of Annex II NIS Directive, namely 1. Energy 2. Transport 3. Banking 4. Financial market infrastructures 5. Health sector 6. Drinking water supply and distribution 7. Digital Infrastructure, two sectors were selected, Energy and Banking. The criteria for the selection include the maturity of cybersecurity standardisation and certification in each sector, the cybersecurity capacity of the sector, the potential societal impact in terms of compromise of cybersecurity,[31] the critical value and effect in cybersecurity. At European level, finance (EU FI-ISAC) and energy (EE-ISAC) were the first two EU Information Sharing and Analysis centres to be established, which illustrates the strong cross-border collaboration aspect in these two sectors. In addition, both sectors were confirmed as interesting case studies after the test interview with the Dutch Standardisation Institute NEN.

In addition, the focus is ICT products/systems and services, in line with the scope of the CSA. Certification of persons and skills is therefore excluded from the study. The report provides a set of policy recommendations to the NCSC, which does not include however an assessment of the potential impact of different roles for the organisation in terms of resources, efficiency, impact on society. Another limitation relates to the ongoing developments at EU level regarding the European Cybersecurity Framework and a ´moving target´ approach. The collection of data for the research ended in June 2020. As mentioned above, the research is limited to accredited conformity assessment bodies, as accreditation is a formal legal requirement in the EU Cybersecurity Act. Finally, the accessibility of information and experts for interviews was hindered, but not impacted by the ongoing conditions during the COVID19 pandemic.

The Report is structured as follows. First the legal frameworks on cybersecurity in the Netherlands and the European Union are presented and analysed in Chapters 2 and 3. Next, Chapters 4-6 depict the cybersecurity certification in the Netherlands, following the EU Cybersecurity Act. Chapter 4 focuses on conformity assessment, and Chapter 6 on the industry (vendors and users/consumers). Next, following the analysis in the previous Chapters, Chapter 7 positions the NCSC in the cybersecurity certification landscape and discusses options for possible roles for the agency. Chapter 8 concludes the Report.

2 Legal Framework on Cybersecurity in the Netherlands and the mandate of NCSC

2.1 An overview of the Dutch Cybersecurity Legislation

The Netherlands is a frontrunner in societal digitization, using digital infrastructure for the communication between citizens and the government, to provide healthcare and education and to increase flexibility and mobility in the workplace.[32] Although this digitization is a driver of economic growth and societal welfare, it is also paired with risks for privacy and data security, cybercrime and the disruption of societal processes through cyberattacks. The government must ensure that there is a high level of protection against cyberthreats and incidents. To strengthen the resilience of the Dutch digital society, the Dutch government has decided to strengthen the legal position of the NCSC in their coalition agreement.[33] Following this decision, the NCSC has been separated from its parent organisation – the National Coordinator for Terrorism and Security (NCTV), to become a standalone organisation. Close ties between the two organisations continue to exist, since a high level of cooperation between these organisations is important to protect the Dutch society from on- and offline threats.[34]

Due to the many aspects of digital security, the Dutch cybersecurity landscape is complex and fragmented, involving many players that focus on different aspects of digital resilience. The tasks and responsibilities concerning cybersecurity are arranged through several laws and policies. Moreover, the Netherlands relies on cooperation between private and public parties.[35] Besides national legislation, there is a growing body of European legislation in this area, and the Netherlands must ensure compliance of its cybersecurity arrangements with the EU law. In 2018, the Network and Information Systems Security Act (Wbni)[36] was introduced to implement the European NIS Directive in Dutch law. The Wbni replaced the Data Processing and Notification Requirement Act (Wgmc)[37] and led to a reorganisation of the Dutch cybersecurity response network. With the upcoming national implementation of the European Cybersecurity Act, the existing division of tasks and roles of existing organisations are due to change again, introducing new tasks and obligations on Dutch public bodies concerning cybersecurity. What follows is a brief overview of the Dutch cybersecurity landscape of the prevailing regulation.

2.1.1 Network and Information Systems Security Act

The Wbni functions with the specific purpose of strengthening the resilience of Dutch cybersecurity. The Wbni is specifically aimed at the prevention of cyber-crises and incidents and promoting the operational information exchange concerning these threats and incidents between relevant national and international entities.[38] The Wbni codifies and allocates the competences, rights and obligations of the CSIRT and sectoral CSIRTs concerning the notification of- and coordinating responses to- cyber threats and incidents. When a cybersecurity incident occurs at an essential service provider, they have an obligation to notify the NCSC as the central contact point.[39] Digital service providers have to notify the Ministry of Economic Affairs and Climate (Telecommunications Agency)[40] via their CSIRT-DSP.[41] Sector specific authorities are also appointed in the Wbni: The Dutch Central Bank (DNB) is appointed as the responsible authority for cybersecurity in the banking- and finance sector; The Ministry of Infrastructure and Waterworks is the competent authority for cybersecurity in the Transport and water distribution sector and the Ministry of Health is responsible for cybersecurity in the healthcare sector. Besides this, the Wbni lays down that any service provider, no matter whether they are essential or fall under a different competent authority, can voluntarily notify the NCSC if they suspect a cybersecurity threat.[42]

Besides this, the Wbni lays down several obligations on the private parties in relevant sectors. Operators of essential, vital and digital services have an obligation to minimize risks by ensuring that cybersecurity technology remains up to date and to take precautions that ensure the continuity of the service in case of cyber incidents.[43] The Wbni provides a general competence for the introduction of general administrative measures[44] that impose further obligations on these service providers to take precautions to minimize the risk of cybersecurity incidents.[45] The Wbni also determines when and how service providers are to notify cybersecurity threats and incidents, detailing the criteria for establishing a cybersecurity threat and what information must be included in the notification.[46]

The Wbni also determines how any processing of data, including personal data, should happen in case of a cybersecurity threat or incident. CSIRTS (or alternative computer crisis teams) and intelligence- and security services are parties that must be informed.[47] The Wbni lays down in which situation the public should be informed, stating that this may happen either by the Ministry of Justice or by the service providers themselves. According to the Wbni, the competent authority may decide that if a cyber-incident occurred at a vital or digital service provider, it is necessary to inform the public.[48] In addition, in relation to supervision, officers tasked with supervision must be appointed by Ministerial decision and these appointments have to be published in the Official Dutch Law Gazette.[49] The Wbni provides the sector specific competent authorities (aside from the Ministry of Justice) with the powers to conduct security audits, give binding instructions, and in case of non-compliance impose sanctions in the form of fines or forced restoration of the rightful situation.[50]

2.1.2 The Ministerial Decision on Network and Information Systems Security

Implementing the Wbni, the Dutch government has also introduced the Ministerial Decision on Network and Information Systems Security (Bbni)[51], further clarifying and detailing the Wbni. For instance, the Bbni establishes which service providers are vital service providers or provide essential services in the Netherlands.[52] Furthermore, the Bbni clarifies how notification of cyber incidents should take place and establishes an exemption for financial institutes with regard to precautionary measures mandated by the Wbni.[53]

2.1.3 The Adaptation law of the Cybersecurity Act

The Cybersecurity Act, being a Regulation, is binding without transposition into the Dutch legal order. An adaptation law is however in the making to facilitate the execution of the Regulation by setting rules on procedures, enforcement, the provision of legal protection and to give instructions to executive authorities in the Netherlands. The CSA adaptation law (Uitvoeringswet Cyberbeveiligingsverordening) is still a draft bill. The law is expected to appoint the Ministry of Economic Affairs and Climate Policy as the national cybersecurity certification authority, and to delegate this role to the Radiocommunications Agency Netherlands.[54] It will also appoint the Accreditation Council[55] as national accreditation body, which will have the right to accredit conformity assessment bodies.

The CSA adaptation Law will set the rules and procedures on distributing certifications with the assurance levels 'basic, substantial or high' in accordance with the Cybersecurity Act. The law will provide the Radiocommunications Agency Netherlands with additional competences regarding the assessment of certifications with a high assurance level by instating the Decision of approval model'[56] Moreover, the law will set out additional optional criteria for a request assessment for cybersecurity certification, supplementing the mandatory requirements set out in the Cybersecurity Act.[57] Furthermore, it will arrange domestic procedures for

legal protection that are in line with the General Administrative Act (Awb).[58] Finally, the law will assign competence to the court of Rotterdam and the College for appeal for businesses[59], a specialised judiciary tribunal in disputes regarding the approval or denial of cybersecurity certification requests.

2.2 Other Relevant Legislation

2.2.1 Dutch Telecommunications Act

The Dutch Telecommunications Act (Telecommunicatiewet) imposes obligations on providers of telephone- and internet access services concerning the creation, operation and commercialisation of communication networks. Besides more operational and consumer-oriented obligations, the Telecommunicatiewet also contains several provisions on the protection of data and privacy and the continuity of services.[60] Especially chapter 11a imposes some obligations that demonstrate overlap with the obligations imposed on them under the Wbni. They need to minimize the risk of threats to their safety and security, ensure continuity and notify the competent authority of any cyberthreats or incidents. Interestingly, the providers of internet access are considered vital service providers under the Wbni, placing them under the supervision of the Ministry of Justice. In the Telecommunicatiewet however, the Ministry of Economic Affairs and Climate is the responsible Ministry. As such, there are overlapping obligations on the providers of internet access services. The Nationale Cybersecurity Agenda (NCSA) clarifies that the obligations on internet access providers as laid down in the Telecommunicatiewet will continue to exist despite the introduction of the Wbni. As such, providers of internet access have a parallel obligation to both Ministries under different laws.[61]

2.2.2 Cybercrime & the Dutch criminal code

The Police Data Act[62] and the Criminal Data Act[63] regulate data processing for the purpose of criminal proceedings. The Dutch Criminal Code (Wvsr)[64] lays down material provisions regarding cybercrime. It incorporates the Computercrime III Act[65] and criminalizes the hacking of computers with the purpose of digital theft or with the purpose of using the computer as a listening- or espionage device, as well as prohibitions for fencing digital products, grooming and provisions to ensure that undesirable photographs or videos can be taken off the internet by court order.[66] The Computercrime III Act extends the investigative powers of law enforcement with regards to cybercrime to include powers to have encrypted files decrypted and allowing police to hack into devices for the purpose of fighting on- and offline crime

2.3 Governance of Dutch cybersecurity protection

The concurrence of the Wbni (following the NIS-Directive) and the forthcoming Implementation Law of the CSA provides synergies in ensuring a high level of cybersecurity in the Netherlands. The governance of cybersecurity in the Netherlands is distributed over a number of entities. Table 2 provides an overview of the various actors and their roles, which is elaborated below.

Entity	Wbni
Ministry of Justice	• Competent authority for legal implementation • Responsible for vital and essential sectors

Ministry of Economic Affairs and Climate Policy	• Competent authority for digital and energy sectors • CSIRT for digital sector through the CSIRT-DSP
Ministry of Infrastructure and Water Management	• Competent authority for transportation sectors and drinking water distribution[67]
Ministry of Health, Welfare and Sport	• Competent authority for Health sector[68]
De Nederlandsche Bank	• Competent authority for the banking sector and financial infrastructure[69]
NCSC	• Central contact point for CSIRTS[70] • CSIRT for vital service providers and providers of essential services[71] • Voluntary notifications[72] • See chapter 2.3.1. for overview of all tasks
NCTV	• Coordinator for the performance of tasks by the NCSC[73]
IBD	• CSIRT for municipalities[74]
Z-CERT	• CSIRT for healthcare services[75]
CERT Watermanagement	• CSIRT for Waterworks[76]
SURFcert	• CSIRT for organizations using SURF webhosting services[77]
Agentschap Telecom (Radiocommunications Agency Netherlands)	-
Dutch Accreditation Council (Raad voor Accreditatie)	-
AIVD	• Has the right to receive information on cybersecurity threats and incidents

Table 2: Overview legal competences of relevant governmental actors in the Dutch Cybersecurity landscape

This table demonstrates that the protection of Dutch Cybersecurity relies on a sector-specific approach in many entities that rely on the coordination of central bodies such as the NCTV, NCSC and the Radiocommunications Agency.[78] Due to this decentralized approach, a high level of cooperation and coordination is required. As such, initiatives such as the Digital Trust Center (DTC) have been created to stimulate cooperation between the NCSC and MinEZK.[79] Cooperation between the NCSC, intelligence services and other relevant public players is facilitated by the creation of the National Detection Network (NDN) and National Response Network (NRN). Similarly, sectoral cooperation is facilitated through the creation of Information Sharing and Analysis Centers (ISACs). [80]

2.3.1 The legal mandate of the NCSC

The NIS Directive lays down an obligation on Member States to adopt a national strategy on the security of network and information systems to achieve a high level of cyber security.[81] The Netherlands has implemented the NIS-Directive by adopting the Network and Information Systems Security Act, appointing the Ministry of Justice (in short: MOJ) as the responsible Ministry. The NCSC is part of the Dutch Ministry of Justice and

Security.[82] Through the Decision on the Organisation of the Ministry of Justice[83] (in short Organisational Decision) – which lays down the division of competences between departments and organisations within this Ministry - the Ministry of Justice has mandated the NCSC with powers and obligations to give proper execution to the Wbni, and with that ensure compliance with EU law.[84] Following the Wbni and Organisational Decision, the NCSC is tasked with the prevention and mitigation of societal disruption deriving from cyber threats and incidents and the strengthening of the resilience of the digital Dutch society.[85] The NCSC previously was part of the NCTV. The Ministry of Justice has decided to provide the NCSC the status of an independent body under their Ministry following the implementation of the Wbni.[86] However, the NCTV is the national cybersecurity coordinator and responsible for Cyber Security and State Threats, providing the NCSC directions as to what services to provide.[87]

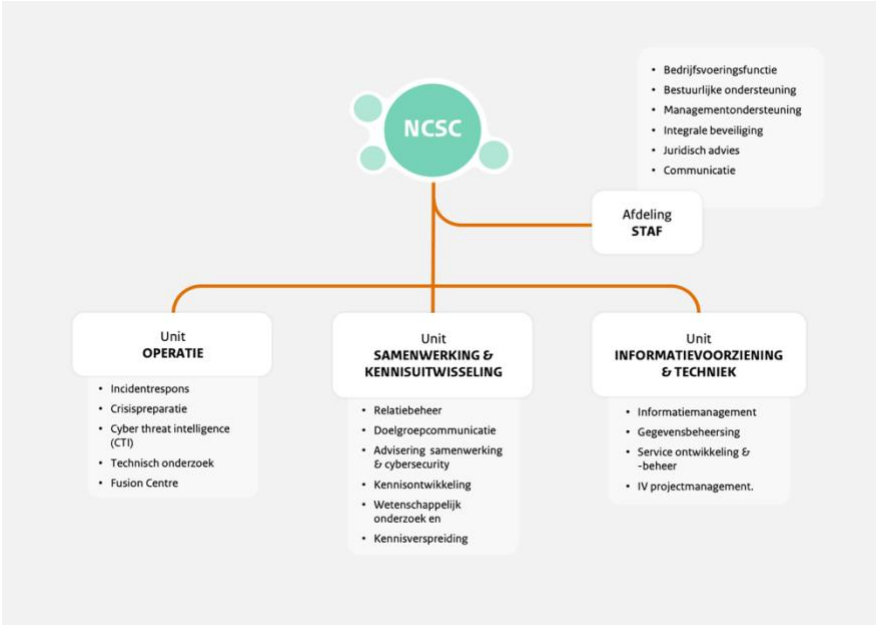


Figure 2: Organisational structure of the NCSC-NL, source: NCSC website

The legal mandate for the powers of the NCSC is mostly limited to tasks required to fulfil their obligations under the Wbni, which have been delegated to them by the Ministry through the Organisational Decision (Organisatiebesluit). Following these laws, the NCSC:

- Is the Single Point of Contact regarding cybersecurity threats and incidents;[88]
- Is the Cyber Security Incident Response Team (CSIRT) for vital service providers of providers of essential services and;[89]
- Is responsible for processing voluntary notifications of cybersecurity threats and informing the relevant parties;[90]
- Provides support to the providers of vital service providers and other providers that are part of the Dutch government to help them take measures to safeguard or restore the continuity of their services;[91]
- Informs and advises vital service providers and other providers that are part of the Dutch government and others within and outside of the Netherlands concerning cyberthreats or incidents involving the aforementioned;[92]

- Conducts technical analysis and research regarding cyberthreats and incidents in order to safeguard or restore the continuity of services and inform relevant players of cyber threats and incidents;[93]
- Disseminates information on threats with organisations that have a responsibility to inform the public, CSIRTs and providers of internet access or internet communication services.[94]

Their role under the Wbni and Organisational Decision places the NCSC in a central coordination role between the Dutch sector specific CSIRTs, Ministries and makes them the international contact point for the Cybersecurity agencies of other Member States.[95] Besides the aforementioned roles, the Organisational Decision makes the NCSC responsible for holding the secretariat for initiatives in private-public cooperation concerning cybersecurity.[96] This role for the NCSC is not mentioned in the Wbni, nor is it mandated by the NIS Directive. However, considering the multiple private parties that play a role in Dutch cybersecurity, the legal mandate for this role may provide interesting opportunities for the NCSC.[97]

2.3.2 Other governmental actors in cybersecurity

Radiocommunications Agency

The Radiocommunications Agency (Agentschap Telecom) is responsible for a broad range of supervision and enforcement activities. This includes (but is not limited to) oversight of the Radio Equipment Directive (RED) 2014/30/EU[98], licensing amateur radio stations and high frequency stations, ensuring the safety of internet connected devices.[99]

As mentioned, the Radiocommunications Agency will be appointed to fulfil the role of the National Cybersecurity Certification Authority (NCCA) for the cybersecurity certification in the Netherlands.[100] It will be granted the powers to request any information needed from conformity assessment bodies, to conduct audits, to take appropriate measures in accordance with national law to ensure conformity assessment bodies or certificate holders to comply with the European Cybersecurity scheme.[101] To enforce their powers, the AT can impose penalties as set out in chapter 5 of the Awb including a lump sum penalty, periodical penalty payments or actual reparation to the rightful state, together with complementary powers that will be introduced with the Cybersecurity adaptation Law.[102]

AIVD and MIVD

The General Intelligence and Security Service of the Ministry of the Interior and Kingdom Relations (AIVD)[103] has a special subdivision that specializes in cybersecurity threats and concerns; the National Bureau for Security Connections (NBV)[104]. The NBV helps to evaluate and develop secure cybersecurity products, has a role in the development of cybersecurity standards and has a potential role in certification. Moreover, a part of the NBV, the National Distribution Authority (NDA),[105] is solely responsible for the registration and distribution of cryptographic devices.[106] Besides this, the NBV holds positions in several international bodies such as the Council Security Committee and the Council Security Committee Infosec that evaluate security products. The NBV evaluates holders of cryptographic devices on behalf of NATO and has a supervisory role in the Dutch Certification Scheme on IT-Security (NSCIB)[107] where the Common Criteria certificates by TÜV Rheinland Nederland can be obtained.[108] As such, the AIVDs role and influence in the Dutch (and international) cybersecurity landscape are significant.

The introduction of the Wbni also has consequences for the powers of Dutch intelligence and security services such as the AIVD and Military Intelligence and Security Service (MIVD).[109] According to the Wbni, any information regarding cybersecurity threats or incidents that is retractable to the victimized organisation can be shared between the NCSC and the AIVD and MIVD if this is required to prevent the disruption of society, or if the NCSC has the explicit consent from the victimised organisation.[110]

Digital Trust Centre (EZK)

The Digital Trust Centre program was set up as a temporary project by the Ministry of Economic Affairs and Climate Policy, and will become a permanent part of the MinEZK after 2020.[111] Its goal is to make Dutch enterprises in non-vital sectors more resilient against cyber-threats. Whilst the Ministry of EZK (AT) fulfils its role as CSIRT through its CSIRT-DSP department, the Digital Trust Centre is a platform for the dissemination of information and knowledge to digital service providers and for applying for subsidies and grants. According to MinEZK, the Digital Trust Centre cooperates extensively with the NCSC: by knowledge sharing between the associated parties, the Digital Trust Centre can rely on the expertise of the NCSC to provide digital service providers with high quality advice on the precautions they are to take and what technical measures to use.[112] Currently, the DTC does not have an underlying legal competence.[113] In the recent evaluation of the functioning of the DTC, the government has identified this as a potential problem in the cooperation between the NCSC and DTC, since the NCSC does not have legal grounds to share information with the DTC. The formal introduction of the DTC into the MinEZK in 2021 may provide a clear scope for the role of the DTC as a part of the Ministry and facilitate better cooperation between the organisations.[114]

2.3.3 Information Sharing and Analysis Centres (ISAC)

The Information Sharing and Analysis Centres (ISAC) are sectoral network initiatives, developed and operating under the lead of NCSC, with the aim to increase digital resilience among the participating organisations. The members exchange information on incidents, threats, vulnerabilities, and best practices in cybersecurity in a confidential manner.[115] ISACs are also developed at European level, with which the national ISAC collaborate. The financial and energy sector ISAC were the first ones to be launched in the Union. In the energy sector, the EE ISAC,[116] has been acknowledged by the European Commission, as a specialised entity promoting cooperation among stakeholders.[117] The European FI-ISAC was founded in 2008 to support exchange of information between banks, CERTs, and law enforcement.[118]

3 Union legislation on cybersecurity certification

3.1 EU Legislation on Cybersecurity

3.1.1 Network and Information Security Directive

The Network and Information (NIS) Directive 1148/2016 lays down measures for the achievement of a high common level of security of network and information systems in the Union. Since 2018, the NIS Directive has been implemented in all Member States with national laws corresponding to the goals set in the Directive. The key pillars of the Directive are:

- The obligation for each MS to adopt a national strategy and designate national competent authorities.
- The establishment of a Coordination Group for the exchange of information among MS.
- The creation of a network of computer security incident response teams ('CSIRT network').
- The obligation for operators of essential services ('OES') and digital service providers to adopt security measures and notify incidents to the competent authorities ('incident notification').

The NIS Directive therefore harmonizes the set-up of authorities in MS, establishes communications and information exchange tunnels, and obliges providers of critical services in different sectors to take measures to prevent, mitigate and address risks and incidents related to network and information security. The essential services are determined in the Directive: energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, and digital infrastructure,[119] however the implementation by MS was recently reported to be quite diverse.[120] Similarly, the types of digital services are also predetermined in Annex III of the NIS Directive (online marketplace, online search engine, and cloud computing service). The obligations of the two types of providers – OES and digital service providers– are not identical, and in that sense, it has been argued that the digital service providers are subject to a 'lightweight' regime in relation to the OES.[121]

To ensure a common approach in terms of security measures to be adopted by OES (Art. 14) and Digital Service Providers (Art. 16), the NIS Directive points at standardisation, and in specific European or internationally accepted standards and specifications.[122] Following this, the European Cybersecurity Agency ('ENISA') published a report mapping the landscape and identifying gaps in standardisation. The ENISA report examined both formal standardisation bodies such as ISO and ETSI, but also informal de facto consortia, the standards of which are well accepted in the market and identified a small number of gaps and some areas of overlap. The NIS areas/obligations for which standards were identified are:

- Risk management for networks and information systems (Art. 14 and 15)
- Impact prevention and minimisation (Art. 14 and 15)
- Computer Security Incident Response Teams (CSIRTs), Competent Authorities, and Single Points of Contact (Art. 7)
- Identification of Operators (Art. 3)

The NIS Directive does not contain specific provisions on certification.

3.1.2 Cybersecurity Act

The new Regulation 881/2019 on ENISA and information and communications technology cybersecurity certification ('Cybersecurity Act') complements the NIS Directive and strengthens the cybersecurity strategy,

coordination, and enforcement of the Union.[123] The Regulation provides an enhanced mandate to ENISA in relation to the previous regime[124] with a multitude of responsibilities and coordination roles, which essentially make the Agency the Union center of expertise on cybersecurity.[125] ENISA is tasked to:

- Contribute to the development and implementation of cybersecurity Union policy and law (Art. 5),
- Assist MS in their capacity building in order to improve prevention, detection and analysis of cyber threats and incidents (Art. 6),
- Support operational cooperation of Union institutions, bodies, agencies, stakeholders (Art. 7),
- And have an active role in the support, development, and implementation of the cybersecurity certification, as explained in the following sections (Art. 8).

In addition, ENISA is given a role of awareness raising, education, technology forecast and analysis on cybersecurity.

The second pillar of the CSA is the introduction of a 'European cybersecurity certification framework' for ICT products, ICT services, and ICT processes. Since modern ICT products regularly integrate third party technologies and components, the Union regulator deemed it significant to ensure that the reliance does not pose additional risks and create vulnerabilities that may affect in turn the security of the ICT products, services, and processes.[126] The overall goal of the introduction of the framework was the increase of the level of cybersecurity by enabling a harmonized approach to cybersecurity certification at Union level.[127] The European cybersecurity certification schemes should ensure that certified ICT products, service, processes, comply with requirements that protect the availability, authenticity, integrity, and confidentiality of data or services.[128]

3.1.3 A closer look at the Cybersecurity Act Certification Framework

A. Essential Components of the certification framework

The Regulation establishes a framework for European cybersecurity certification, which is a mechanism for the establishment of European cybersecurity certification schemes.[129] The certification schemes provide requirements on the basis of which the level of cybersecurity of an ICT product, or ICT process, or ICT service may be assessed.[130] The schemes to be established under the European cybersecurity certification framework need to be designed to achieve a minimum number of security goals, provided in Art. 51 CSA, such as for example:

- Protect data against accidental or unauthorised 1. storage, processing, access or disclosure[131]; 2. Destruction, loss, alteration, or lack of availability.[132]
- Only authorised persons, programs, or machines access the data, services or functions.[133]
- Security by default.[134]

Type of component	CSA framework	CSA Provision
Object of certification	ICT products, ICT process, ICT services or groups thereof	Rec. 73
Type of conformity assessment	• Third party certification • Conformity self-assessment by manufacturer or provider also possible for low complexity/low risk situations with EU statement of conformity	Rec. 79 Rec. 80 Rec. 82 Art. 53 Art. 56

Voluntary/mandatory	Voluntary in principle, mandatory also possible in MS	Rec. 91 Rec. 92 Art. 56
Geographical scope	Only Union level, no national certifications under the CSA[135]	Art. 57
Minimum scheme content	Yes, provided in the CSA	Rec. 84 Art. 51
Mutual recognition	Yes, throughout the Union. (Peer review system across national cybersecurity certification authorities)	Rec. 73 Rec. 99
Granularity	Three assurance levels (basic – substantial - high) for certification. Conformity self-assessment: only basic Evaluation levels also possible	Rec. 77 Rec. 86 Rec. 88 Art. 52 Art. 56
Transparency	Website with schemes maintained by ENISA National authorities notify COM on accredited conformity assessment bodies Penalties in national laws notified to COM	Rec. 85 Art. 50 Art. 61 Art. 65
Supervision & enforcement	By national cybersecurity certification authorities	Rec. 73 Rec. 102 Art. 58
Consistency	European Cybersecurity Certification Group (ECCG)	Rec. 103
Revision	Every 5 years, evaluation by ENISA	Art. 49

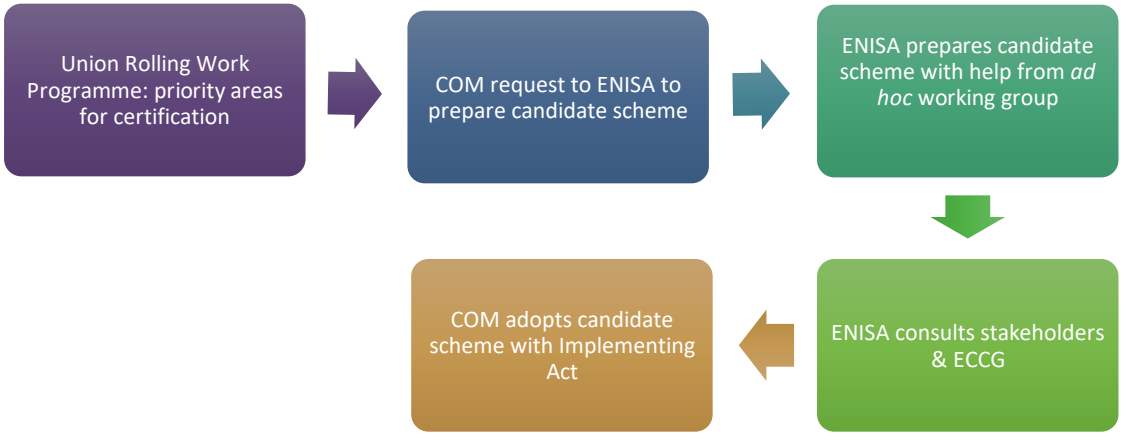
Table 3: Overview of key elements of the CSA certification framework

To better determine the level of assurance of the European cybersecurity schemes, the Regulation provides for different assurance levels that correspond to the level of risk associated with the intended use of the ICT product, ICT process, or ICT service.

While the framework primarily refers to third party conformity assessment (certification), it does allow for conformity self-assessment.[136] That is the case for low risk ICT products/process/services, for which the manufacturer or provider may make a self-assessment and issue an EU statement about the fulfilment of a given CSA scheme. The basic essential elements of the European cybersecurity certification schemes are not left at the discretion of the scheme drafters, but a thorough non-exhaustive list of minimum components is provided in the Regulation.[137] This ensures that all the schemes will have a common structure and address common significant issues. The schemes are European, and 'replace' national ones, in the sense that the latter cease to produce effects.

B. Governance of European cybersecurity certifications

The European cybersecurity certification framework follows a multi-stakeholder model. The initiative of requesting candidate schemes lies mainly with the European Commission. The initiative is based on a work program for European cybersecurity certification ('Union rolling work programme for European cybersecurity certification'), which announces on an annual basis the Commission's strategic priority for schemes. As Figure 2 shows, the Commission requests ENISA to prepare a candidate scheme, ENISA then has the obligation to prepare a candidate scheme. In some cases, the Commission or the ECCG may request the preparation of a candidate scheme that is not part of the Union rolling work programme, in which case ENISA is not obliged to accept the request. There are several embedded guarantees in the procedure to ensure the quality and acceptability of the scheme. One of them is the mandatory establishment of ad hoc working groups by ENISA, which are tasked to provide specific advice and expertise for each candidate scheme.[138] In addition, when preparing the scheme ENISA has to consult all the relevant stakeholders, such as standardisation bodies and industry.[139] A third guarantee is the task of the ECCG to provide expert advice to ENISA for the preparation of the candidate scheme, as well as an opinion once the candidate scheme is drafted.[140] Once the candidate scheme is finalised, ENISA submits it to the Commission, which in turn may adopt the candidate scheme as European cybersecurity certification scheme with an implementing act.



Once the implementing act adopting a European cybersecurity certification scheme is published, it can

Figure 3: Overview of adoption of candidate European cybersecurity certification scheme

become operational. Conformity assessment bodies may be accredited to provide services based on the scheme and interested parties may apply for certification. The entities that may apply for certification are of two types: manufacturers and providers of ICT products/services/processes. The accredited conformity assessment bodies are allowed to conduct the process for schemes with basic or substantial assurance level (Art. 56 (4)). By exception, private conformity assessment bodies are allowed to issue certificates with a 'high' level of assurance only with the approval of the national cybersecurity certification authority. The latter may itself also provide certification by way of derogation from the rule that CABs provide such services.[141]

C. The role of national cybersecurity certification authorities

The national cybersecurity certification authorities are the cornerstones of the implementation of the schemes. While they also participate in the preparation phase, for example via the ECCG, their most significant role concerns the phase after the candidate schemes are adopted by the Commission. There are one or more national authorities in each MS, designated as the national cybersecurity certification authorities, with a multitude of tasks and powers pertaining to monitoring and enforcement. The powers and tasks of the national cybersecurity certification authorities may be grouped in the following categories:

Powers and tasks related to bodies offering conformity assessment

Actively support and assist the National Accreditation Bodies (NAB) in monitoring and supervising the activities of the conformity assessment bodies, providing expertise and relevant information to the NAB.[142]

- Request conformity assessment bodies to provide any information they require for the performance of their tasks.[143]
- Obtain access to premises and carry out audits of CAB to verify compliance.[144]
- Monitor and supervise public bodies offering conformity assessment.[145]
- In cases of certification schemes with specific or additional requirements, the national cybersecurity certification authorities may provide authorisations to conformity assessment bodies to perform such tasks, or restrict, suspend, or withdraw such authorisations.[146]
- Handle and investigate complaints about certificates issued by national cybersecurity authorities or conformity assessment bodies, or about EU statements of conformity.[147]
- Take appropriate measures to ensure CAB comply with the Regulation or a European cybersecurity certification scheme,[148] impose penalties and require the immediate cessation of infringements of the obligations set out in the Regulation.[149]

Powers and tasks related to manufacturers and providers

Issue certificates, in case a European cybersecurity certification scheme, requires it in a duly justified manner and by way of derogation to the rule that CAB issue certificates.[150]

- Supervise and enforce the compliance rules in the certification schemes or the EU statements of conformity in case of self-assessments.[151]
- Request holders of cybersecurity certificates or EU statements of conformity to provide any information they require for the performance of their tasks.[152]
- Obtain access to premises and carry out audits of holders of cybersecurity certificates or EU statements of conformity to verify compliance.[153]
- Take appropriate measures to ensure holders of cybersecurity certificates or EU statements of conformity comply with the Regulation or a European cybersecurity certification scheme,[154] impose penalties and require the immediate cessation of infringements of the obligations set out in the Regulation.[155]

Quality monitoring of issued certificates

Withdraw European cybersecurity certificates issued by national cybersecurity certification authorities or CAB, in case they don't comply with the Regulation or a European cybersecurity certification scheme.[156]

- Monitor relevant developments in the field of cybersecurity certification.[157]

Cooperation, information sharing, and notification obligations

Cooperate with other national cybersecurity certification authorities, other public authorities, and the Commission. This obligation includes sharing information about non-compliance of ICT products/processes/services with the CSA Regulation or the requirements of certification schemes,[158] and sharing good practices regarding certification and technical issues.[159]

- Notify the Commission of the conformity assessment bodies authorised to provide certification with specific or additional requirements per Art. 60(3)[160] and request the Commission to remove a CAB from the list.[161]
- National cybersecurity certification authorities should be subject to peer review by the equivalent authorities of other MS.[162]
- Provide an annual summary report to ENISA and the ECCG.[163]
- To avoid the potential conflicts of interest from the different type of tasks and powers (for example issuing certificates and monitoring bodies offering conformity assessment), there are strict obligations for separation of the activities. To safeguard the integrity of the processes and reliability of the schemes, the activities of the authorities should be carried out independently from each other.[164] In practice, independence may be guaranteed by legal, financial, and organisational separation of the groups or authorities within a MS that conduct activities with a risk of function creep and conflict of interest.

3.2 Other relevant legislation

3.2.1 The Radio Equipment Directive

The Radio Equipment Directive (RED) provides requirements for radio equipment in order to be placed in the market and put into service. The Directive is a harmonized law, thus lays down only the essential requirements to be met by the equipment, and the further specification of how entities comply with those requirements is provided by harmonized technical standards.[165] Radio equipment is highly dependent on cybersecurity, as vulnerabilities or malicious attacks may compromise the achievement of the requirements set by the law, and in practice render such equipment harmful to the health and safety of individuals.[166]

3.2.2 The Regulation on non-personal data flows

As of May 2018, the Regulation on non-personal data flows applies in the Union.[167] The Regulation aims at ensuring that non-personal data flow freely in the Union, are available to authorities and can be ported. In relation to portability of data, the Regulation urges the Commission to facilitate the development of self-regulatory codes of conduct, especially covering:[168]

- Best practices for switching service providers and the porting of data in a structured, commonly used and machine-readable format.
- Minimum information requirements to be provided to professional users before a contract is concluded.
- Awareness raising.
- Approaches to certification schemes that facilitate the comparison of data processing products and services for professional users.

Taking the reference to certification schemes, the European Commission already submitted a request to ENISA to prepare a candidate scheme for cloud services.[169]

3.2.3 The General Data Protection Regulation

The General Data Protection Regulation introduced a novel certification framework ('data protection certification mechanisms'),[170] for the purpose of demonstrating compliance with the provisions of the Regulation.[171] Certification in the GDPR is voluntary, and its territorial scope both national and European. The object of certification is one or more data processing operations, and the certification process is conducted by either data protection authorities or accredited conformity assessment bodies. The subject matter of the data protection certifications under Art. 42 and 43 may be either all-encompassing, in that it covers data controller or processor obligations stemming from the entirety of the Regulation, or issue specific. The issue-specific certifications may focus on specific aspects of compliance with the legal requirements such as data protection by design and by default or security of data processing.[172] In fact, ENISA has already identified the close link between the Union information security legislation and practices and security of data processing in Art. 32 GDPR.[173] In that sense, despite the different approach of the certification frameworks in the CSA and the GDPR, bridges could be established at least concerning baseline data security elements, such as evaluation of threat occurrence, risk evaluation, security measures, and others.[174]

4 Dutch Cybersecurity Certification Landscape: conformity assessment bodies

4.1 Objectives and approach

This chapter provides an overview of the certification landscape in the Netherlands. By certification landscape, we mean the key market actors, with a focus on the providers of conformity assessment and especially certification services,[175]. This Chapter also includes a section on Public Private Partnerships, due to their significance in shaping cybersecurity best practices and requirements in the Netherlands.

4.2 Standardisation

The national standardisation body NEN, is active in the field of cybersecurity primarily in standards development, which is the core business of NEN, but also has an evolving role in certification scheme management. There are several NEN Technical Committees which deal with aspects of cybersecurity, including information security, such as the NEN Committee on Information security, cybersecurity, and privacy, as well as several sector specific ones such as the NEN Committee on Financial Services.[176]

4.3 Conformity assessment bodies

4.3.1 Accredited v. non-accredited certification bodies and testing facilities

Accreditation enhances trust to the conformity assessment as it confirms that accredited conformity assessment bodies are competent in terms of expertise but also integrity and independence to perform assessments and award certifications. The Cybersecurity Act makes accreditation for cybersecurity a formal obligation. The CSA requires that certification bodies providing European Cybersecurity certification are accredited by the National Accreditation Body, the RvA in the Netherlands.

There is wide range of certification bodies and testing labs operating in the Netherlands. The number of conformity assessment bodies which are formally accredited by the RvA in the field of information security and cybersecurity, however, is relatively limited. While the European Cybersecurity certifications are not yet published, it is noteworthy that many certification bodies already have the intention of getting accreditation for their services.

4.3.2 Domestic and supranational activity

Certification bodies in the Netherlands are oriented towards the local market, but often they are branch of a larger group of certification bodies either in the form of a network or they belong to the same group of companies, with offices and locations in different Member States or even worldwide. This has an impact towards a series of issues. One is that while the Dutch market is the target, the preferred standards and certification schemes are international or European ones. There are of course exceptions, when there is a need for a national standard, such as for example the NEN 7510 on information security in the healthcare sector, which is a broadly used standard. Another consequence is the orientation towards collaboration not only with the Dutch regulator at large, but also – if not primarily – the European institutions such as the European Commission and ENISA. Certification bodies are interested to follow the EU CSA developments and participate in the development of the upcoming cybersecurity certification schemes, for instance by joining the ENISA *ad hoc* working groups.

4.3.3 Outsourcing v. internal resources

The outsourcing of the evaluation process is not uncommon. The interviewed organisations explained that they sometimes collaborate with smaller organisations with expertise in complex technical assessments and licensed labs performing penetration and other tests. Other organisations opt for utilizing the resources of establishments in other countries, belonging to the same mother company. It was reported that smaller organisations lending their expert auditors, might be interested to provide certification services autonomously themselves in line with the EU cybersecurity certification schemes such as the EU Common Criteria scheme. This is an interesting CSA aftermath, which is expected to re-arrange such collaborations, and thus impact the landscape at large.

4.3.4 Other relevant activities

Several of the conformity assessment bodies in the Netherlands belong to organisations that also offer consultancy services on cybersecurity to their clients. Some organisations explicitly abstain from activities other than conformity assessment to ensure that any conflict of interest is presented. Those however that offer consultancy services take measures against conflicts, such as separating the units and personnel working on consultancy and those working on evaluation and certification in different legal entities. Obligations on taking measures with regard to impartiality stem from the ISO/IEC 17065 standard which is the foundation for accreditation of conformity assessment bodies. More specificly, certification bodies are not allowed to be the same legal entity with consultancies, designers, manufacturers or service providers.[177]

4.3.5 Drivers and obstacles for cybersecurity certification

Achieving a high cybersecurity level in a product, system or service is one of the evident drivers for cybersecurity certifications. Even more, the demonstration of an assessment by an independent certification body adds to trust and reliability. Reputation with partners and consumers is another strong driver. A competitive advantage (first-mover advantage) is also reported to be a driver, especially when certification responds to consumer expectations.

It is also often the case that larger companies require cybersecurity certifications, such as the ISO/IEC 27001, of their partners and suppliers. This is the case for example when manufacturers ask from the providers of product components to provide evidence of the level of security, in the form of cybersecurity certification. In the domain of critical infrastructures, the OES in the Netherlands require their suppliers to be certified, which stems from the OES duty of care imposed by the Wbni. However, certification is not mandatory, just an often-preferred option.

Legislation is reported to one of the main drivers for certification. Compliance with a legal requirement to be certified was unanimously raised in the interviews with conformity assessment bodies for this Study.

In the Netherlands, the National Cyber Security Agenda (NCSA), which has set the objectives of cybersecurity in the Netherlands for the forthcoming years, stated that the Netherlands aspires to be ´at the forefront of digitally secure hardware and software´ (Ambition nr. 3). To achieve such a goal, the NCSA recognises that standards and certification make an important contribution to the digital security of hardware and software.

In fact, the NCSA refers to the option of mandatory certification for specific product groups in the short term[178] and a gradual compliance with a CE mark type of seal for all Internet-connected products in the long run.[179]

Conformity assessment bodies are in favour of mandatory certification, not only from a commercial point of view, but also because in their view it will harmonise and raise the security level of products, systems or services. One

interviewed expert explained that when consumers buy a piece of technology, they need to know what the security level of this technology is, which is something that can be verified with certification. Apart from the consumers, who however, are not always aware of what CE marking for example stands for, B2B relations could also benefit from mandatory certification, which would replace the private security assessments currently taking place on an *ad hoc* basis.

Other indirect ways of semi-mandatory nature are also a strong driver for companies to get certified. Participation in procurements is an example of such semi-mandatory certification.

When it comes to the obstacles, the ratio of costs with added value is brought up as a hindering factor. Certification is increasing the price of the product, which is one of the reasons why manufacturers might not be willing to certify their products. For some companies, the correction of non-conformities after the assessment by the certification body is reported to be quite costly. Another obstacle is liability. As one of the interviewed certification experts explained, even if certification is not a legal requirement, it does create liability for the company that applies for it:

> *"Once a company applies for certification, the evaluation and any non-conformities are proof that the company is not in line with the standard."*

The result of the conformity assessment is formally recorded on paper, which according to the experts, creates responsibility for the management of the organisation. This is the case despite the fact that the evaluation reports are not published or communicated to the government or the public; the management of the organisation has to act on defects when informed in any manner, including an evaluation report of a certification process.

4.3.6 Relation and role of the NCSC

Conformity assessment bodies and the Dutch Standardisation Institute are not direct partners with the NCSC. Those organisations have collaborated in several occasions with the NCSC and overall value its expertise and knowledge.

The interviewed standardisation experts from NEN acknowledge the significance in NCSC participating in the NEN standardisation committees. Despite not having a formal collaboration at the moment, they recognise that the participation of NCSC in the standardisation committees allows NCSC to represent the interests of its stakeholders. NCSC is working on critical sectors at the moment, and standards are being developed in those sectors. Interviewed standardisation experts highlighted that cooperation with governemental organisations such as the NCSC are helpful for identification of areas in need of standardisation and certification.

Conformity assessment bodies are interested to collaborate with the Dutch authorities, and view positively roles such as information sharing, awareness raising and publishing information about certified entities. In other countries and on a European level, several interviewed CABs are involved actively in shaping developments, via participating in working groups or via engaging in consultation. Some CABs are interested to assist the NCSC in giving training on cybersecurity certification, should it decide to take on such an activity in the future. Apart from any role in certification, some CABs would like to see the NCSC have an active role in standards development, which is a view shared by NEN, as mentioned above.

4.4 Public Private Partnerships and certification

A number of strategic Public Private Partnerships with a focus on cybersecurity play a significant role in the field, raising the competitiveness of the country in the field. Developed bottom-up, the PPPs aim at bringing the collective resilience capacity at its maximum, in place of individual efforts. Within the framework of their goals, PPP sometimes engage with specifications development and certification. The market players in the Netherlands, often choose to be partners of national and European PPPs. This series of initiatives show that the Netherlands relies on significant input and involvement by private parties, addressing multiple facets of cybersecurity development.

Some examples, are:

- **Partnering Trust**, an initiative of the Ministry of Economic Affairs, aims at creating uniformity in IT requirements of cloud and other service providers through the development of reference frameworks for participating organisations. Participating organisations are established also in Germany, France, and Luxembourg.[180]
- The **Dutch Secure Software Alliance (SSA)** aims at ensuring that software security is guaranteed from an early stage in production of an IT-product, and that the security is safeguarded in every step of its life cycle of a product. In order to ensure the quality of products, the SSF relies on the Centre for Information Security and Privacy Protection's (CIP) Secure Software Development Framework.[181]
- **Cross Sector Cyber Test Bed (CSCT**), which is a cross-sectoral platform that allows different sectors to exchange test results of cybersecurity testing to develop new standards and norms for cybersecurity.
- The **Zeker-OnLine** mark aims to make online service providers safer for users. Zeker-Online provides assessments in cloudhosting software for (i) salary administration, (ii) childcare and (iii) accountancy. Currently, Zeker-Online has ten participants with a certified cloud application.[182] Zeker-Online is also a part of Partnering Trust.[183]
- The **Dutch Payments Association**, a sector specific PPP, provides certification services of POS terminals (POI devices), based on its own scheme. The scheme sets out conditions for suppliers and manufacturers of POI devices. The POI certification is mandatory for the members of the Dutch Payments Association.
- The **European Network for Cyber Security (ENCS**), a PPP in the energy sector, focuses on the deployment of secure critical energy grids and infrastructure. Dutch energy companies such as ENEXIS and STEDIN, as well as Netbeheer Nederland – the branch organisation for all the energy grid management companies in the Netherlands- are members of ENCS. The ENCS both develops whitepapers and other documents with cybersecurity requirements for its members, but also maintains a test lab, which has the capacity to test against security requirements. The ENCS lab works with its own ENCS requirements, but also external normative sources for requirements such as the Oesterreichs Energie requirements catalog for end-to-end security for smart metering and the Dutch Smart Meter requirements.[184] The procedure includes a documentation review, a functional testing, robustness testing, and penetration testing. The ENCS does not award certification.

5 Dutch cybersecurity certification landscape: vendors and users

5.1 Market overview

The Netherlands is often reported to have a strong competitive cybersecurity market, composed mainly of Small Medium Enterprises which provide innovative specialised products and services.[185] Large international enterprises are also active in the Netherlands, responding mainly to the need for provision of services to Dutch multinational companies. The multitude of companies active in the field, as shown in Figure 3 draws a picture of a diverse market. Cybersecurity service providers and consultants support organisations by analysing and mitigating threats, conducting risk and crisis control, providing advanced solutions. Another range of services in the field relates to mobile services, secure cloud services, and infrastructure services. Software providers represent another segment of the landscape, as well as ICT manufacturers. In specific, there are companies with several products in an area of specialisation such as encryption products, secure identification authentication and digital signing solutions, but also mono-liners, specialising on a single product.[186] From studying the landscape, it is well understood that the companies offering cyber-security services provide preventive and incident, threat and attack response services. Another type of company that emerged as active in the field is insurance companies, providing compensation for financial loss, and other services such as PR repair of the company and individual reputations.[187]

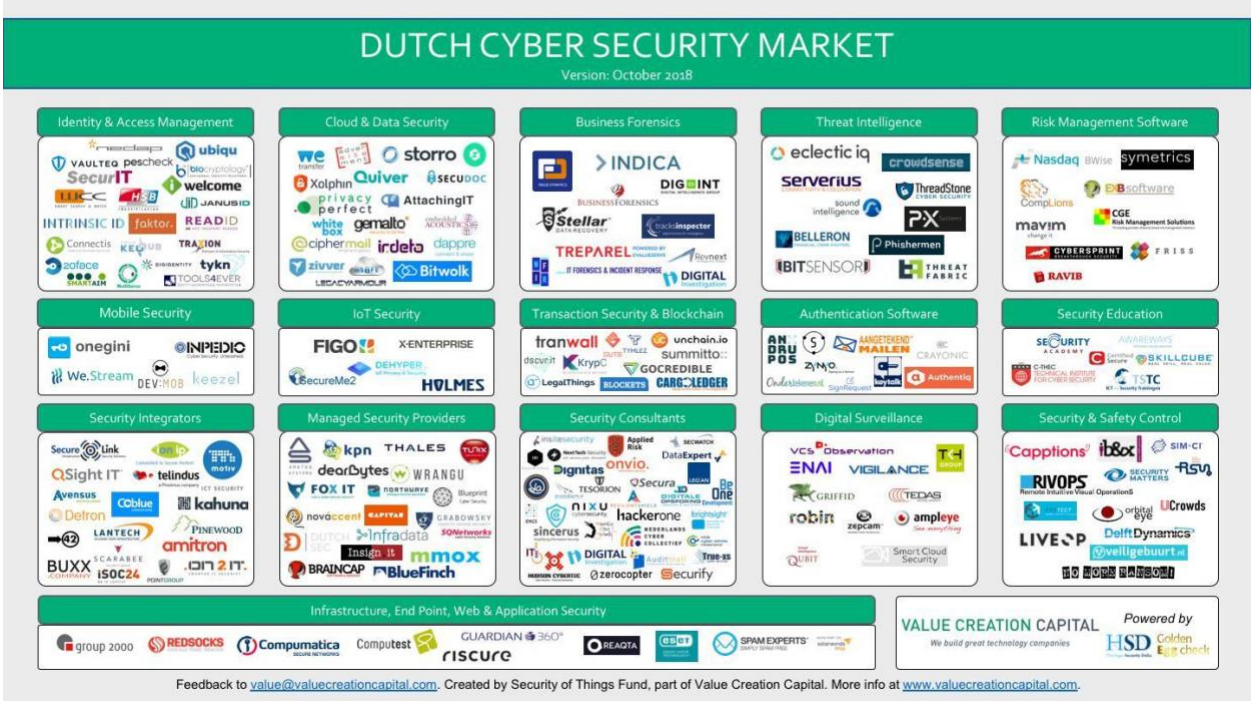


Figure 4: The Dutch Cybersecurity market (2018)[188] according to Value Creation Capital

The question is how many of those organisations investing in cybersecurity consider cybersecurity certification valuable for their business and their supply chain and are actively seeking to get certifications in the field. The Cybersecurity monitor 2019, published by the Statistics Netherlands (CBS), reports a number of cybersecurity measures undertaken by companies in sectors such as energy, healthcare, ICT. The measures range from implementing antivirus software to risk analyses, encryption, VPN and authentication with software or hardware

tokens.[189] Adherence to standards or certification are not included in the measures, even though some of the measures could be informed from available technical standards. In fact, it became quite clear from the interviews conducted in the course of the report that it is not seldom that companies consult or conform to standards, but choose not to pursue certifications. Second party conformity assessment is also used often instead of certification. Vendors or service providers require their supply chain to conform to standards, and this is verified by auditors of the vendors, instead of a certification party. This seems to be a faster (and cheaper) solution than certification, without however much recognition from other third parties.

Despite the above issues, certification services in cybersecurity seem to provide a dedicated market share for certification bodies in the Netherlands, one that is expected to grow following the developments in legislation with the Network and Information Security Directive, the Wbni and most recently the Cybersecurity Act.

5.2 Case study I: the energy sector

5.2.1 The Dutch energy sector in a nutshell

The key energy actors are transmission system operators ('TSO'), distribution system operators ('DSOs') and energy suppliers.[190] TSOs and DSOs are network operators, responsible for network construction needed for safe and security transportation of energy, while energy suppliers directly provide consumers with gas and electricity.[191] The network operators are under the supervision of the Dutch Authority for Consumers & Markets ('ACM').[192]

Type of actor	Energy	Actor
Transmission system operators	Gas	Gasunie Transport Services
	Electricity (onshore)	TenneT
	Electricity (offshore)	TenneT
Distribution system operators	Gas	Cogas infra & beheer – Enduris – Enexis – Liander-RENSO – Stedin – Westland - Zebra
	Electricity	Cogas infra & beheer – Enduris – Enexis – Liander-RENSO – Stedin – Westland

Table 4 overview of TSO and DSO in gas and electricity the Netherlands

The Netherlands has a competitive market of energy suppliers for gas and electricity, with more than thirty suppliers such as Eneco, Engie, Nuon, Essent, Delta Energie, Energiedirect and Greenchoice. [193]

Furthermore, the Nederlandse Aardolie Maatschappij ("NAM") is responsible for onshore and offshore exploitation of oil and gas, and the Netherlands Petroleum Stockpiling Agency ("COVA")[194] is responsible for the management and supervision of strategic oil stocks.[195]

Following the NIS Directive and the Dutch transposition law, a number of actors are appointed as Operators of Essential Services (Vitale aanbieders). Both TSOs and DSOs in electricity are currently considered as OES. The scope of OES might be extended in the future to include electricity producers. Gas includes additionally the only exploration and extraction company in Groningen.[196] As regards oil, COVA is the OES. The national competent authority responsible for the OES in the energy sector in the Netherlands is the Dutch Telecommunications Agency (Agentschap Telecom).

With regard to the legal framework, the main national laws regulating the energy sector are the Electricity Act 1998 (Elektriciteitswet 1998)[197], the Gas Act (Gaswet)[198], the Heat Act (Warmtewet)[199] and the Independent Network Management Act (Wet onafhankelijk netbeheer).[200][201] The Dutch Electricity Act and the Gas Act lay down the responsibilities of TSOs and DSOs. Both entities have the duty to safely and efficiently transport and distribute electricity and natural gas. They are also tasked with the creation and maintenance of connection points that are linked with consumers and other networks.[202] The Independent Network Management Act ensures that network operators are not allowed to carry out any activities other than the management of electricity and gas networks. The national legislation is in line and complemented with the European legal framework on energy, such as the regulations establishing the European Network of Transmission System Operators for Electricity ('ENTSO-E') and the European Network of Transmission System Operators for Gas ('ENTSO-G'). [203]

5.2.2 Activities in cybersecurity

Cybersecurity is clearly on the agenda of all respondents in the interviews. Guaranteeing uninterrupted energy delivery is the core business of TSO, DSO and energy producers. The energy network, distribution nodes, switches (the OT environment), but also office IT used for billing, HR, CRM, etc and IoT devices installed at customer's home (smart meters, smart thermostats, energy monitors, etc) are vulnerable to attacks and other disruptions.

The main focus of cybersecurity measures relates to making sure the entire operation meets basic cybersecurity requirements. The foundation here is the ISO/IEC 27000 series. All respondents are fully aware of these standards and their companies either (informally) adhere to standards in these series or are certified according to these standards. The ISO/IEC 27000 series is considered to be the most important set of standards in the energy sector.

Depending on their specific activities, TSO, DSOs, electricity producers and equipment manufacturers deal with specific standards. For instance, smart meters have to conform to NTA 8130, for OT-security ISA99 and IEC 62443 are relevant.

The energy sector is fairly specific in terms of hardware, there are few of the shelf components that can be deployed in the energy grid. Custom solutions will have to be developed in most cases coming from a relatively small set of suppliers. Cybersecurity requirements, consequently will also often have to be developed for specific equipment or projects. Many DSOs are members of the ENCS (European Network for Cyber Security). This platform plays an important role in developing these custom requirements as well as developing (ad-hoc) standards. The ENCS members actively engage in these processes and have access to the ENCS industry standards. ENCS also tests components and assesses conformity of these components with the requirements.

5.2.3 Drivers, needs, and trends in cybersecurity certification

Certification is expensive because it involves a rationalisation of internal procedures and processes, documentation, external audits, assessment and out of pocket costs for the CAB conducting the audits and providing the certification. This explains why, although the value of ISO/IEC 27000 are indisputable, not all entities in the energy sector go through the process of formal certification.

A reason to become formally certified is that this may be a legal requirement to operate in a certain market. Due to the German legal certification requirements, an energy provider is ISO/IEC 27000 certified for its German operations, but not for its Dutch.

Mandatory certification is deemed desirable by all respondents, some have drawn a parallel with the GDPR; without the GDPR, privacy and data protection would be much lower on the agenda. Having said that, determining the required level of certification will not be straightforward. IEC 62433, for instance, defines multiple security levels. The lowest level guarantees protection against low-skilled hackers while the highest level protects against advanced state actors. Currently, organizations are free to choose which level they want to adhere to. The market has not (yet) decided for itself what the minimum security level should be. A mandatory minimum level security level for the critical infrastructure could be desirable to create an adequate level playing field.

Another reason to make certification mandatory is that adoption of standards and certification is a slow process. Making certification mandatory may help guide industry in the direction of higher cyber security standards. Costs and benefits of certification are, however, difficult to predict and it may be too costly for small organisations to comply. This makes the decision to mandate cybersecurity certification difficult.

A driver for some to adopt certification in the industry is that it demonstrates to supervisory authorities (Data Protection Authority & AT) and market supervisory authorities (EZK & ACM) that cybersecurity risks are actively mitigated.

Certification also allows parties operating in the energy field (e.g. Siemens) to show the market they comply with a certain standard (e.g. IEC 62443 for OT equipment). They have a commercial interest in being certified. It allows them to distinguish themselves and it helps in tender processes where customers have many requirements. Being certified for certain aspects helps ticking the requirement boxes of these customers.

From the perspective of buyers of equipment, certification of the supply chain is relevant. Standardization helps them compare between multiple vendors and to consider the security of products and services provided by suppliers. For the suppliers, it will also be easier to prove they comply with certain standards if they are certified. With regards to OT, some parties draft their own requirements/standards which suppliers must comply with, which go further than ISO/IEC 27001.

The respondents from the energy critical infrastructure try to push suppliers towards certification, but the players in the Dutch energy market are relatively small and thus have limited market power to persuade big international suppliers. Industry platforms (ENCS, ENSTO-E) are used to leverage the power of like-minded companies to further standardisation/certification. Collaboration in these European platforms is also important because equipment is bought on an international market and European solutions are deemed desirable to ensure the devices are of adequate quality and security.

Drivers	Needs	Trends
Improve security of internal processes (through adoption of ISO/IEC 27000 series)	Raise company internal awareness of importance of cybersecurity	(relatively slow) (informal) adoption of standards
Build trust with consumers (smart thermostats) through certified IoT devices	Have trustworthy certification schemes available	
Improve cyber security by requiring suppliers to be certified		
Demonstrate compliance to regulator	Clarity on (legal) requirements	
Comply with mandatory regulation (in Germany)	Create level playing fields and raise cybersecurity	Increasing call for making certification mandatory
Increasing scope of certifiable products/services and submitting these to testing/certification	Expertise to cover specific technologies	Evolution of private standard setting and testing initiatives such as ENCS

Table 5: Drivers, needs and trends in cybersecurity certification: Energy sector

5.2.4 Relation with and role of NCSC

The entities in the energy supply chain have regular contacts with the NCSC, for instance through the Energie ISAC, particularly to exchange information regarding threats and incidents. The NCSC is seen as a trusted communications partner regarding operational cyber security.

Some entities also have contacts with supervisory authorities, such as AT regarding equipment regulated under the Telecommunications Act and Data Protection Authority for GDPR related concerns.

All respondents remark that they prefer NCSC to maintain their role as a platform for 'informal' information exchange. NCSC is seen as a trustworthy entity that facilitates cross sector cybersecurity information. Any move towards giving NCSC a role in enforcement would jeopardise trust in NCSC. Their role is seen primarily as a knowledge centre for very specific affairs that they can share with the sector. They have insight in threat intelligence on a national and international level that goes beyond that of any player in the energy sector.

The NCSC also have many contacts with foreign (government) entities that one cannot really expect from commercial enterprises.

NCSC is seen by some as being engaged in standardisation. One respondent sees a potential role for NCSC on a European level mapping out the needs for the development of standards in conjunction with European ISACs and ENISA. ENISA has good deliverables of a high quality and it would be good if such detailed deliverables are also issued for the Energy sector, perhaps NCSC could have a role to play in that regard. Another respondent stated that as NCSC also has specific guidelines/ standards about information security, it could engage in norm-setting but in an advisory rather than supervisory role.

NCSC is considered knowledgeable with regard to the office IT-environment, but less so when it comes to the SCADA-environment.

Furthermore, a role for NCSC is seen in clarifying the impact of the CSA since there is still a lot of uncertainty about this as well providing a roadmap on how to proceed in the next few years.

There seems to be consensus amongst our respondents that NCSC should maintain the role it has right now: facilitating and coordinating on operational cyber security and leaving oversight and enforcement of the various obligations to the supervisory authority: AT. Conversely, when it comes to handling incidents and exchanging knowledge and information, the AT should not be involved, but keep this function with NCSC. The AT is seen as the (future) supervisory authority that is involved ex post to control/ supervise what has happened.

5.3 Case study II: the banking sector

5.3.1 The Dutch banking sector in a nutshell

The Dutch banking market mostly consists of several large domestic banks. This high level of concentration in the Netherlands is – at least in part – a result of past policies that have led to the disturbance of competition in the market, which have incentivized banks to grow and to specialize further. Due to this high level of concentration, the banks in the Netherlands are relatively large and well organized, for instance through private associations such as the 'Association for Dutch Banks' (NVB[204]) and the 'Dutch Payments Association' (BVN), in which also other payment providers are represented.[205] On the European level, associations such as the European Banking Frontier (EBF) allow for representation and cooperation on the European level. Moreover, the banks are under the supervision of the Dutch Central Bank (DNB) and the Authority Financial Markets (AFM[206]) on a national –and the European Central Bank (ECB) and European Banking Authority (EBA) on a European level.[207]

Type of actor	Services	Actors
Banks	Financial services	ABN AMRO; Amsterdam Trade Bank; Binckbank; BNP Paribas; De Volksbank; ING; Interbank; Rabobank; Van Lanschot; foreign banks; other small domestic banks
Associations	Representation and cooperation	NVB; Betaal
Supervisors	Supervision and compliance	Dutch Central Bank; European Central Bank; Authority Financial Markets; International Monetary Fund

Table 6: Overview of key actors: Banking sector

In principle, supervision on the financial stability and reliability of Dutch banks will happen by the DNB. The supervisors at DNB assess the suitability of high executives in banks, granting permits, combating financial-economic crime, and checking whether institutions are financially strong so that they can deal with any crisis. There is an exception however: the ECB supervises banks that hold an exceptional share of European capital. Due to the size and concentration of the Dutch market, the ECB directly supervises Dutch banks such as the ABN AMRO; BNG Bank; Coöperatieve Rabobank UA; de Volksbank; ING Groep etc. As such, Dutch banks are under the shared supervision of the Dutch Central Bank and the European Central Bank. Finally, on a global level the International Monetary Fund (IMF) can conduct periodical reviews of the financial stability of the Dutch financial markets. Besides supervising financial stability, the AFM supervises the way in which banks treat their customers and how they cooperate in the Dutch financial market. The supervision by the AFM is aimed at the protection of consumers and to increase consumer trust.

In order to regulate the Dutch banking sector, Dutch banks rely on a combination of domestic and European laws. On the domestic level, the reliability of Dutch banks is arranged through the Financial Supervision Law (Wft[208]). This law is supervised by DNB. Moreover, the Dutch financial institutions are bound by the Law for the Prevention of Money Laundering and Financing Terrorism (Wwft[209]), the Law on the Supervision of Trust Funds (Wtt[210]) and the Sanctions Law (Sw[211]). These laws ensure the integrity of the Dutch financial system, the prevention of crime and the punishment of illegal behaviour respectively. The Wtt is under the supervision of the DNB, the Wwft is supervised by the AFM and other authorities and the Sw is supervised jointly by the DNB

and AFM. On a European level, banks are bound by legislation such as the Payment Services Directive 2 (PSD2), to ensure access to consumer data by innovative payment services.[212]

5.3.2 Activities in cybersecurity

Important legislation concerning cybersecurity in the banking sector are the Wbni on the domestic level and the NIS-Directive (and soon the CSA) on a European level. Under the Wbni, the DNB has been appointed as the responsible authority for dealing with cybersecurity threats- and incidents in the banking sector. Banks that encounter cybersecurity threats will notify this to the DNB and AFM, which in turn will determine whether the NCSC and ENISA need to be informed. As such, financial institutions are subjected to overlapping notification obligations in cybersecurity incidents between cybersecurity and financial authorities. Moreover, banks are already required to demonstrate a high level of security – including cybersecurity – under their existing legal obligations towards the Financial Supervision Law (Wft). The law imposes a general obligation on banks to provide due diligence concerning the safety of consumer finances (zorgplicht).[213] The AFM periodically assesses whether financial institutes meet these obligations, including whether cybersecurity is sufficiently safeguarded. The AFM expects 'robust' security measures for cybersecurity from the banks. In order to ensure that they meet this high level of protection, banks may rely on generally accepted information security frameworks such as the ISO/IEC 27001 norms and the NIST CSF frameworks, or PCI norms for the distribution of payment cards.[214] However, following their obligations to the AFM, banks are free to choose how they fulfil their due diligence obligation. This allows for heterogeneous approaches to cybersecurity whilst not excluding innovative solutions. It is for this reason that the respondents in the interviews believed that cybersecurity is sufficiently safeguarded in the Netherlands, and that extensive mandatory certification schemes would not be desirable. However, respondents do believe that voluntary certification schemes imposed on their commercial partners in IoT, Cloud and other digital products may be beneficial for commercial interests. This type of certification would allow banks to demonstrate the security of the products they acquire towards the Authority for Financial Markets, and may be a selling point for the providers of cybersecurity products.

5.3.3 Drivers, needs, and trends in cybersecurity certification

The main drivers for obtaining cybersecurity certification in the Dutch banking sector in general are primarily to demonstrate compliance with the due diligence obligations that they have towards the supervisory authorities. However, the respondents in the interview argue that certification in itself is not required to provide this guarantee of a high level of security. In fact, certification of the banks is considered to demonstrate a proper organisation of management processes, rather than ensuring a high level of security overall. Banking services actors however value cybersecurity certifications, since the market for cybersecurity products is marked by a high level of newcomers with heterogeneous products. As such, certification is important to the extent that it helps banks identify reliable trading partners. Respondents do note that certification should not be too restrictive or costly, since this may hinder the provision of innovative products by start-ups, or drive suppliers of low cost products out of the market due to the costs of compliance. As such, respondents strongly prefer voluntary certification rather than mandatory certification, since this allows for heterogeneity in both the offered products and the providers offering them. Besides the commercial benefits that certification may provide in trading with the providers of cybersecurity and IoT products, European standards may facilitate cross border business flows between banks. Certification ensures that banks from different EU (or global) countries adhere to the levels of

cybersecurity protection desired by Dutch banks. Due to the rapid developments in the proliferation of new cybersecurity products and the regulation of cybersecurity in the banking sector, European certification may help to clarify and harmonize the rules concerning cybersecurity in banking sectors of different Member States. The drivers, needs and trends in cybersecurity can be summarized as follows:

Drivers	Needs	Trends
Identification of reliable trading partners	Voluntary certification, should allow a high level of heterogeneity	Certification schemes are being developed for IoT and Cloud
Cross-border cooperation and business flows between banks	Cross-border harmonization; certification on European level	There is an increasing intensity of European legislation on cybersecurity
Demonstrating compliance with legal obligations	Clarity on rules of the certification scheme	Increasing compilation of various standards and norms through certification schemes

Table 7: Drivers, needs and trends in cybersecurity certification: Banking sector

5.3.4 Relation with and role of the NCSC

Regarding the NCSC, interviewed organisations consider the NCSC to have a high level of expertise and an important role in facilitating contact between different partners in cybersecurity and the dissemination of information. Moreover, one of the respondents argued that the operational role of the NCSC is fulfilled well, that they would prefer if the scope of their operational role was extended to include non-vital sectors as well. Another view was that the powers of the NCSC in responding to cybersecurity threats should be extended, allowing the NCSC to take more decisive action. However, none of the respondents see a role for the NCSC as a certification authority for two reasons:

the NCSC is seen as an excellent knowledge partner, and the role of certification authority would result in a conflict of interest between a support and supervision task and;

the NCSC may not have the organizational capacity to fulfill a certification role. However, one of the respondents does note that the NCSC could provide an important role in collecting information on all European requirements concerning cybersecurity and help (financial) institutes with implementing measures to comply.

6 State of the art and new developments in standardisation and certification

6.1 Introduction

This chapter offers a snapshot of the most commonly used standards for conformity assessment in cybersecurity, as shown in the literature and the empirical research conducted for this Study. It also depicts the latest developments with regard to the Cybersecurity Act and elaborates on views of the Dutch cybersecurity certification stakeholders on the potential impact from an organizational and operational perspective.

6.2 Standards

6.2.1 Formal standards as key component to certification

The research for this study, including the interviews and information received from conformity assessment bodies, points at the direction of formal standardisation from international, European, and national standardisation bodies being a key component to existing certifications in the field of cybersecurity. Unlike other fields where requirements and criteria for certification are often drawn by other sources such as the law,[215] standards are essential for cybersecurity certifications. Formal standards, developed by the recognised standardisation bodies, have a particularly significant role to play in relation to harmonised legislation, such as the Radio Equipment Directive, which covers aspects of security, but also to the forthcoming CSA certifications.

6.2.2 Non-formal standards and SMEs

Not only formal standards developed by the recognised standardisation bodies,[216] are used as a foundation for certification. Also specifications developed by specific individual (or groups of) vendors may impose their own conditions to respective partners and hence act as standards for compliance. Furthermore, a certification procedure against a recognised standard requires extensive documentation in addition to testing, which is reported to raise the overall costs for obtaining the certification.

As a result, some conformity assessment bodies opt to offer certification services also for non-formal standards, when for example a client has low risk processes or is a start-up or a Small Medium Enterprise (SME). This is an interesting connection with the possibilities introduced in the CSA for self-assessment in low risk cases and the option of manufacturers to issue declarations of conformity.[217]

6.3 Cross-sector cybersecurity standardisation and certification

While there are a multitude of technical standards in the market, the standards used for accredited conformity assessment in cybersecurity, as shown in this Report, are a handful. The standards, which are pivotal to cybersecurity and cybersecurity certification in specific, originate mostly from international standardisation bodies, and to a lesser extent, European ones. The cybersecurity standards used in conformity assessment relate to products, management systems and services. While there are sector specific standards adopted by organisations,[218] a characteristic example of which is the banking sector, the most common ones are generic, sector-neutral standards. In some cases, initiatives developing a sector specific specification on the basis of a generic standard were mentioned during the interviews, as a best practice worthy of attention. An example of such a standard is the NEN 7510, which is the adaptation of the 27001 to the healthcare sector information security needs in the Netherlands.

6.3.1 ISO/IEC 27001: Information Security Management Systems

By far the most commonly used standard from conformity assessment bodies and their clients is the ISO/IEC 27001 standard on information security management. The ISO/IEC 27001 establishing, implementing, maintaining and continually improving information security practices in organisations. The standard is reported to deal with complex IT systems, assessing each organisation in context. Further, its security-by-design approach, which requires the information security management system to be integrated with the organisations' processes and management structure already from the design of processes, systems, and controls, is considered one of its strong assets.[219] Oftentimes, conformity to the ISO/IEC 27001 is a requirement imposed by industry actors to their supply chain partners, especially in the critical infrastructure domain. Certification in line with the ISO/IEC 27001, apart from the benefits it might bring to the information security of an organisation, is also an element of trust. It should also be noted that ISO/IEC 27001 may include additional components in a certification process, such as the requirements based on the ISO/IEC 27018 on cloud computing or the ISO/IEC 27701 standard for privacy information management.[220]

6.3.2 Common Criteria: Product Certification

The ISO/IEC 15408 is an international standard used for IT security evaluation. Common Criteria, allow in brief, a product developer to tailor an evaluation to the security needs of its product, by choosing an Evaluation Assurance Level (EAL). The 7 available Evaluation Assurance Levels, which stand for different tests, reflect a granular approach, also followed in the European Cybersecurity Act, despite with less assurance levels.

Achieving a high EAL and receiving certification for it, boosts trust in a product, and is often required, by counterparties before entering into commercial collaboration agreements.

Common Criteria certification is often connected to both commercial and reputation benefits. Apart from a competitive advantage it might offer, it is perceived as reflecting quality and reliability. While organisations recognize that the higher the EAL is, the more costly the process, they are willing to go through certification. This does not apply for Small Medium Entreprises and start-ups.

In the Netherlands, TÜV Rheinland Nederland is currently appointed by the AIVD to administer the Dutch Common Criteria scheme (NCSIB)[221] and provide certification services. TÜV Rheinland collaborates with different evaluation facilities in the Netherlands.

6.3.3 IEC 62443 on Cybersecurity for Industrial Automation and Control Systems

The IEC 62443 standard series provides a framework to address security vulnerabilities in industrial automation and control systems (IACS). The standards are applicable to all sectors. IEC 62443 series adopt a quite broad scope including security of "computers, networks, operating systems, applications and other programmable configurable components of the system." The standards also cover SCADA (Supervisory Control and Data Acquisition) systems, which are commonly used by critical infrastructure organisations. The 62443 standards complement ISO/IEC 27701, and follow a modular approach, adapting to the different organisations, making it a flexible framework, which also explains its broad adoption. Conformity to the IEC 62443 is seen as demonstrating the status of digital resilience of an organisation as a whole.[222]The standard series is mentioned in the proposal for a Common Regulatory Framework on Cybersecurity of the United Nations Economic and Social Council[223]

6.3.4 Other specifications

Cryptography standards are also among the commonly used standards, however not for certification. An example is the FIPS 140-2/ISO 19790 standard on security requirements for cryptographic modules.[224]

Informal standards and technical specifications not developed by the formal standardisation organisations, play a role due to the speed of development of the specifications, in combination with the deep knowledge of technological advancements. An example of the Network Equipment Security Assurance Scheme (NESAS), which provides a security baseline to evidence that a network equipment satisfies predefined security requirements, covering areas such as software integrity protection, information management vulnerability, and security by design.[225] Other specifications are the result of the collaboration of multiple standardisation actors in a given technology or use case such as the 3GPP in the telecommunications technologies, which is a partnership among seven telecommunications standard development bodies.[226] Additional examples provided during the interviews were the SANS TOP 20, which is a set of critical security controls for Cyberdefence,[227] and OWASP specifications and guidance.

6.4 Sector specific initiatives in standardisation and certification

6.4.1 ETSI 303 645: Internet of Things and cybersecurity certification

While the current study does not have a particular focus on Internet of Things standardisation and certification, the research revealed that IoT cybersecurity is a rapidly emerging field for conformity assessment. The Dutch Standardisation Institute actively joins standardisation activities in the international and European arena through the national committee members of its IoT Security and Privacy Committee, in which organisations from different sectors such as the banking sector, conformity assessment, research and the regulator, participate.[228]

A prominent example of ongoing standardisation work in the field of IoT, which is likely to be a reference point for conformity assessment activities is the recent ETSI work on Cyber Security for Consumer Internet of Things, providing baseline requirements.[229] As one interviewed expert stressed: "Safety is impossible without cybersecurity. It is impossible to think about any of the IoT devices without thinking about cybersecurity. This is one of the main reasons why we focus on the cybersecurity of the IoT devices."

The standard is reported to aim at allowing vendors that lack experience in cybersecurity to implement the requirements of the standard.[230] Furthermore, ENISA has identified the draft ETSI EN 303 645 standard as a basis of a potential candidate European cybersecurity certification scheme on smart home IoT devices. [231]

In brief, the current version of the draft European Standard (EN) purports to combine good security practices. The draft EN provides baseline requirements that are outcome-focused, so that the means of achieving a given requirement are left to the organisations conforming to the standard. Furthermore, ETSI is currently developing a technical specification (ETSI TS 103 701) to be used by testing labs and certification bodies assessing consumer IoT products against the provisions of the EN 303 645. The technical specification is also intended as an input to a future European Cybersecurity certification scheme on this topic.[232]

6.4.2 Banking sector and energy

The banking sector, including banks, is a very well-regulated sector. Several standards are recommended by the European Banking Authority and the European Central Bank on a range of topics, including cybersecurity. There are several international standards followed by the organisations active in the sector, as well as European harmonised standards. Apart from the cross-sector standards such as the ISO/IEC 27000 series, the Cybersecurity framework from NIST and COBIT standards, sector-specific standards are often linked to Union legislation such as the Payment Services Directive.[233] Banks also follow the PCI Security Standards Council's standards, such as the PSI standard for card distributors and other non-formal standards such as the ORX Reference taxonomy for operational and non-financial risk.[234] Conformity to standards is often not certified. Nevertheless, when organisations in the sector opt for certifications, it usually relates to products and systems, especially technologies, since such certifications reduce information asymmetries between software providers and software users.

The energy sector uses the above standards, such as the ISO/IEC 27001, the IEC 62433 and others. Another standard mentioned in one of the interviews is the NTA8130 on smart grids, which is a Dutch national standard, currently withdrawn. In general, the network operators in the Netherlands follow the same standards for Smart Meters, in line with guidelines from the Netbeheer Nederland. In IT security however, each operator has its own IT security and selects to which standards it conforms. Furthermore, the requirements of the European Network for Cybersecurity were mentioned as an example followed by Dutch network operators. Those however are not followed by certification. The suppliers need to be certified usually against ISO/IEC 27001 to meet the requirements met by the energy company.

6.4.3 Commission requests to ENISA for preparation of candidate schemes

There are currently two ongoing initiatives for development of European cybersecurity certification schemes on the basis of the Cybersecurity Act. One scheme concerns ICT product certification, and the other concerns services certification.

With regard to the product certification scheme, the European Commission requested ENISA to prepare a scheme in line with Art. 48 (2) CSA. The aim of the candidate scheme will be to serve as a successor to the existing Senior Officials Group Information Systems Security (SOG-IS)[235] Mutual Recognition Agreement (MRA). The aim is to both respect the successful aspects of the current SOG-IS MRA, such as authorizing both certification bodies and testing laboratories, but also improve other aspects in line with the CSA, such as by introducing a maximum validity period of certificates.[236]

The future EU Common Criteria scheme (EU CC) will address necessary requirements as provided in Art. 54 CSA and will also provide a mapping to the security objectives outlined in the Cybersecurity Act. In addition, the EUCC will include certification of Protection Profiles. Other issues addressed are recommendations for further guidance and the maintenance of the scheme, competences of skills of auditors, on spot audits and peer assessments, requirements for design.[237] A significant element is expected to be the definition of conditions for the promotion of the certified products, such as the introduction of an easily recognizable seal and a QR code associated with issued certificates.

The European Commission also requested ENISA in line with Art. 48 (2) CSA to prepare a candidate certification scheme on cloud services. The scope of the cybersecurity certification scheme is requested to address:

- Stimulation of the uptake of cloud services among users.

- User trust to cloud services and the provision of cloud services by service providers.

The candidate scheme is intended to consider the guidance and work of the Cloud Service Provider Certification (CSPCERT) Working Group, a platform of private and public entities, supported by the European Commission.[238] In addition, the scheme is envisaged to further support data mobility and compliance with the EU legal framework on non-personal data flows and the General Data Protection Regulation.

Basic	Substantial	High
Shows an intention from the Cloud Service provider to implement security controls	Shows the correct implementation of security controls	Shows the effectiveness of the controls implemented
Deals with simple known attacks	Deals with known attacks by actors with limited means	Deals with complex attacks using SOTA techniques
Document review	Functional testing	Pen testing
Entry level, low risk applications	Core level with real guarantees for mainstream applications in all fields	Strong guarantees, for critical issues in sensitive cases

Table 8: Assurance levels in the candidate cloud services cybersecurity certification scheme[239]

The candidate scheme follows the terminology established in the ISO/IEC 17788, and covers infrastructure, platform, and application.[240] It is designed to be horizontal, in the sense that it defines baseline controls applicable to all services, and can be reused and refined in vertical schemes.[241]

6.5 Impact on the Dutch Landscape

The Cybersecurity Act influences the Internal Market, and inevitably every Member State. While it is still early to assess the impact of the CSA on the Dutch cybersecurity certification landscape, several CSA provisions are expected to have direct and indirect impact on the identified cybersecurity certification actors. The direct impact is rather evident: a national cybersecurity certification authority vested with several related powers will be designated, provisions such as the standstill obligation of Art. 57(1) CSA will priotise European cybersecurity certifications over national ones, and others. The indirect impact, which is the focus in this section, is linked to the stirring of the market that is expected to occur with the development and adoption of the European cybersecurity certifications. Market players will have to make a decision on whether to be engaged with the new certifications, either by offering or consuming certification services.

6.5.1 Conformity assessment bodies

Conformity assessment bodies, including testing labs and certification bodies, are following the developments at European level or -to a smaller degree -participate in those. The core business of CABs offering services on the basis of the standards and specifications discussed earlier in this Chapter is not expected to change dramatically, according to the interviewed experts. Commonly used standards such as the ISO/IEC 27001 are developed in a

manner that are flexible enough to account for regional laws and developments. In addition, the first Commission requests showed an intention to take on board existing best practices, such as the Common Criteria, which will add to a smooth adaptation of CABs, which are already familiar with Common Criteria evaluations.

> *If you read the new regulation [CSA], it is quite easy to find many new services. The CSA covers IoT, Cloud Services, e-health records, qualified trust service providers.*
>
> *[interviewed conformity assessment expert]*

Several certification bodies consider the cybersecurity framework as a good business opportunity and intend to expand their services to the European Cybersecurity certification schemes, once published and available. This includes applying for accreditation for those schemes. Some certification bodies are even interested to shape the developments via for example the ENISA *ad hoc* working groups or by participating in the committees of the national standardisation body NEN. On top of certification services, CABs may also offer trainings and information sessions.

Some CABs also show hesitation. This relates to how successful the European cybersecurity certification schemes will be in practice, and whether there will be market demand for those new certifications. In that case, a more passive stance is adopted, that monitors the developments and waits to see their actual value and use in practice. The fact that the CSA schemes will be based on a law, does not necessarily mean, according to an expert, that there will be demand. The certification mechanisms of the General Data Protection Regulation was brought as an example, as according to the expert "there was a lot of discussion, but the market for certification is close to zero."

> *It is better first to develop a national scheme. It lacks at the moment; we are missing a lot of opportunities to secure the country.*
>
> *[interviewed cybersecurity expert]*

Furthermore, concerns were voiced about the speed with which developments at Union policy making level occur, especially considering the speed with which cyber threats are spread. Those concerns point at the direction of Dutch national schemes, at least until the Union schemes are available. Another expected impact relates to the current collaboration among certification bodies and other organisations providing auditor or testing expertise to the CBs, as it is likely that more bodies will be interested to get accredited and provide certification services for the new schemes. Thus, former collaborators in that case will become competitors, and current CBs will have to find other ways to complement their resources in terms of expertise in order to maintain their market position.

It should be kept in mind that while we are speaking of the 'Dutch' certification landscape, the stakeholders – both in terms of conformity assessment bodies and the industry – often belong to multinational mother companies. This sometimes (but not always, as seen above) changes the perspective of the focus being on the domestic situation. For example, one interviewed expert from a certification body said "We are interested in international and European developments more than national ones, as we are a multinational company with many locations globally."

Another issue relates to the management of certification schemes. A reliable certification scheme needs to be properly maintained, updated, and managed. NEN is currently growing in this role of scheme operator, and it positions itself as an independent organisation, with close touch with the market. Those are both essential elements for a certification scheme. Indeed, as seen in the CSA legal analysis, while the preparation and publication of the candidate schemes is centralized at EU level, with ENISA and the European Commission as key actors, the operationalization and governance of the schemes is rather left at the MS.

> *The important question with certification schemes developed at European level is "who is going to manage it?" Because once you have delivered the scheme, it needs to be maintained. It is a living thing.*
>
> *[interviewed standardisation expert]*

6.5.2 Industry

The banking sector in the Netherlands is informed on the latest developments on European cybersecurity from the European Banking Federation, the Dutch Central Bank, the Dutch competition authority (ACM) or other organisations within the sector.

Experts from the interviewed organisations find that the banking sector is not a priority for a candidate European cybersecurity certification scheme, and because this is a very well regulated market, the uptake of voluntary CSA certifications will be limited in this sector. Interviewed experts argued that the uptake of voluntary certification would mostly be driven by compliance consultancies, as happened with the ISO/IEC 27000 standards. There will likely be a significant impact in the market in general in areas linked to the banking sector, such as cloud, 5G, and IoT. Especially in IoT, certifications will drive companies to invest more in cybersecurity measures. At the same time, IoT CSA certifications will offer some structure on how to deal with such product security issues in complex financial institutions. The banking sector expects that the cost of conformity to CSA certifications might drive out of the market some smaller parties, which are currently offering products for low prices. Concerns are voiced about the new certifications and possible over the top rigid assessment methodologies, as those might hinder innovation in the market.

As regards the energy sector, the Cybersecurity Act does not have full impact yet on the cybersecurity agendas of the interviewed energy companies. It is seen as a stimulus for standardisation and mandatory certification. A push towards standardisation and (mandatory) certification from Brussels – in place of nationally instigated - is generally welcomed by the respondents because of the international and European market. Policy on cybersecurity certification will have to come from the European level, while the operational part in relation to cybersecurity certification should be managed on a national level. Alignment is important, it would for instance be undesirable for a German electricity OES to be certified under ISO/IEC 27001, while the Dutch counterpart conforms to the NIST Cybersecurity framework.

7 Inventory of Potential roles for the NCSC

7.1 Introduction, approach and explanation

The following sections outline an inventory of potential roles for the NCSC in the evolving cybersecurity certification landscape in the Netherlands. The potential roles stem from the building blocks of this report: the analysis of the current legal framework on cybersecurity certification in the Netherlands including NCSC's legal mandate, the new 'opportunities' created by the EU Cybersecurity Act and relevant legislation, and the research on the status, needs, trends, drivers and obstacles, of the stakeholders in the Netherlands, as gathered from the desktop and empirical research.

Each option is presented as follows: First, there is a short description of the background and rationale of the 'role'. Then, the specifics of the role are fleshed out with suggestions on how to move forward or grow further in an already existing role, followed by an explanation and a summary table.

The roles are classified as: 1) **S**upportive 2) **R**eactive and 3) **P**roactive.[242] The supportive roles lay down functions for NCSC which do not place the NCSC at the forefront, but presuppose work in the background, providing advice and support to other stakeholders. The reactive roles are mostly functions where the NCSC acts when requested, as response to an incident or an application for example. The proactive roles are functions that the NCSC plays a central pivotal role in taking decisions and initiatives. It should be noted that the option of 'no role' in the landscape is also a realistic scenario. However, this section reflects on a range of options in reaction to the legal framework and the stakeholder needs and drivers, as identified in the research for this study.

Given that the NCSC has a very specific legal mandate, the main focus is on roles of a supportive/reactive nature. The roles that do not fit in the current mandate of the NCSC do not intend to suggest a structural change of the regulatory landscape, but are reported as an outlook for further research. Furthermore, this section should be seen as a thought provoking exercise that will stir discussion on the future positioning of the Agency in the changing landscape. As mentioned in the scope and limitations of the Study in the Introduction, an assessment of societal impact or organisational and capacity considerations within the Agency is not in the scope of this Report. Last, this is not meant to be an exhaustive systematic analysis, and the roles provided in this section should not be seen as recommendations for the NCSC, but as possible directions that NCSC or other parties could pursue to strengthen cybersecurity through certification mechanisms.

The six roles elaborated below are:

- Role 1: Facilitator of knowledge sharing (supportive role)
- Role 2: Awareness raising and training (supportive role)
- Role 3: Provide assistance to the national cybersecurity certification authority in its tasks (supportive/reactive role)
- Role 4: Provide knowledge and expertise during accreditation of certification bodies (reactive role)
- Role 5: Contribution to development of standards and certifications (reactive role)
- Role 6: Develop own scheme (proactive role)

Role 1: Facilitator of knowledge sharing (supportive role)

Background. The NCSC currently plays a role of providing a cybersecurity collaboration platform. This role is performed mainly through the Information Sharing and Analysis Centres (ISAC). While the NCSC is holding the secretariat, the ISACs are a shared responsibility with the industry participants (for organizing meetings, etc.), providing a structured but flexible governance model. The interviews with the energy and banking sectors showed that dissemination of information and partner consultation are strong points of NCSC's current functioning, a role in which the Agency can grow further. The NCSC is seen as a trusted partner, facilitating the exchange of information among the participants of each ISAC.

The current voluntary incident reporting by actors outside the vital sector could expand in terms of range of relevant topics and partners. As it was mentioned during an interview, the division between vital and non-vital sectors starts to become obsolete. Information coming from non-vital sectors can be useful to vital sectors, and vice versa. In this sense, knowledge should be exchanged further than the direct partners of the NCSC, to a broader circle of partners and collaborators. Since the NCSC mandate is limited to vital sectors, the broadening of partnerships can be done on a voluntary basis, and in collaboration/coordination with other competent authorities.

Possible ways to grow.

A. Expansion in terms of range of topics. In growing in its role as facilitating information exchange and collaboration, best practices and tools for cybersecurity, the NCSC could serve as an information platform for new developments and updates regarding cybersecurity standards and certifications obtained by its partners. A similar role is maintained by several other cybersecurity authorities or agencies in other countries:

- The Centre for Cybersecurity Belgium, coordinates the security evaluation and certification of information and communication systems,[243]
- In Luxembourg, there is a dedicated objective in the National Cybersecurity Strategy to maintain an inventory of standards and good practices in different sectors.[244]
- In Italy, the agency publishes guidelines, standards, best practices and taxonomies in order to facilitate information sharing.[245]

This function may include developments on European Cybersecurity certification schemes and can have a double function: to inform the Dutch market players about the latest developments, and inform other MS about the cybersecurity certification landscape in the Netherlands. This is not to suggest that the NCSC would play a role of consultancy, advising its partners on how to implement certifications. The role under discussion in this section rather relates to an 'information hub', similar to roles of the agencies of other countries, as seen in the examples above.

In collaboration with the AT in its forthcoming capacity as the national cybersecurity certification authority, this role could expand even more as the NCSC could be the designated public registry holder for European cybersecurity certifications. Such a registry could maintain public information on:

- All the published European cybersecurity certification schemes;

- The accredited certification bodies in the Netherlands that offer certification services in line with the EU Cybersecurity Act, their scope, specialization. This can also be done in collaboration with the National Accreditation Body (RvA);
- The details of certification holders (company details, certificate and summary of evaluation report, expiry date of certificate, etc.) and other information, similar to the website intended to be maintained by ENISA (Art. 50 CSA).

B. Expansion in terms of partners. While sector-specific ISACs and in general, collaboration platforms of that type bring a value to their participants in being sectorial, as they address the particularities and specific needs of the sector, there is a reported missed opportunity from not sharing information across sectors. Working in sectors fosters working in silos, whereas valuable information such as about ransomware, could help prevent incidents in other sectors.

This cross-sector exchange could also be useful in the domain of the European cybersecurity certifications. Information on the implementation of the baseline requirements of an IoT or a cloud services scheme, for example, is valuable in all sectors. Even more, if a European cybersecurity certification scheme would become mandatory, either with a national or a Union act, the sharing of information, experiences on implementation, strengths or weaknesses among certification holders would be strengthening compliance with the scheme rules.

Apart from the vital sectors, organisations such as standardisation bodies, conformity assessment bodies, and the National Accreditation Body would also benefit from the type of knowledge shared within the various collaborations of the NCSC. Such partners could join such partnerships as 'observers', learning from the latest developments and updating their own *modus operandi* and especially evaluations, risk assessments, use cases etc. At the same time, this would potentially bring added value to the industry participants, learning from the experience of conformity assessment bodies that work cross-sector and in different countries. Informally, this role can be seen as a capability and capacity building exercise in terms of conformity assessment in cybersecurity in the Netherlands.

In Luxembourg, the national standardisation body ILNAS, has formally been assigned a role in the National Cybersecurity Strategy in helping with information sharing about standards.[246]

Discussion. In holding the secretariat of existing ISACs, the NCSC already has the network and the know-how to expand such collaborations cross-sector, or even with new formal partnerships with conformity assessment bodies. The expansion of the current role of facilitating information sharing on cybersecurity certifications is justified within NCSC's current mandate, because standards and certifications are best practices and tools used among NCSC's partners. This is also the case for expanding NCSC's voluntary collaborators to include conformity assessment bodies. The CSA offers the opportunity for growing in this role, since the law requires monitoring of relevant developments in the field of cybersecurity certification (Art. 58(7)(h) CSA). Nevertheless, if the NCSC would take on a formal role as being the designated public registry holder for European Cybersecurity certifications, this would require strong collaboration with the AT. An alternative option for the NCSC is to maintain such a registry in a more informal manner for the purposes of informing the AT as national cybersecurity certification authority, and not NCSC's partners or the public.

S	Supportive role

#1	Facilitator of knowledge sharing	
Options	a. Expansion in terms of topics	b. Expansion in terms of partners
Strengths	• Information sharing about best practices and tools (: standards and certifications) within the mandate • On a voluntary basis broadening of collaborations within the mandate[247] • Making use of in-house knowledge and experience	
Opportunities	• Helping current partners with useful information • Establishing new networks of collaborators • Creating a niche by connecting conformity assessment bodies with industry.	
Obstacles/Risks	• Potential overlap for the European CSA certifications with the mandated role of the AT (: formal registry keeper) • Information needs to be accurate and up to date if published in a registry.	

Table 9: Overview of Role #1 key aspects

Role 2: Awareness raising and training (supportive role)

Background. The added value of cybersecurity certification is not always clear to the market. Certification bodies explain that the main driver for a company to be certified is an obligation imposed by law. This shows clearly that the benefits of trust, reliability, due diligence, accountability, and primarily the increase of security level in the certified product, process or service verified by an independent third party audit, are often overseen. Some consulted experts note that (cybersecurity) standards are slowly adopted and that the sector (energy) could benefit from faster adoption of new standards and certification schemes. Reasons for not adopting new standards are that the standards in themselves are relatively recent, the cost of implementing and subsequent certification are relatively high, and that cost/benefit ratio is unclear. NCSC can mitigate some of these factors by raising awareness and providing neutral information about the benefits of certain certifications for different sectors and thus contribute to the uptake of European cybersecurity certifications.

Possible way to grow. In this role, the NCSC can educate companies established in the Netherlands about the impact of the European Cybersecurity certification schemes in each sector and how to navigate through the complex standards landscape. In addition, the different options offered by the CSA, monitored self-assessments and certification, should be explained.

A starting point can be the critical infrastructure and vital sector companies, for which there are already established communication channels. Other companies could benefit from such activities. For such companies with an interest in cybersecurity certification and standardisation in other sectors, awareness raising could be done together with other governmental agencies such as the Digital Trust Centre. In this effort, the national standardisation body and the conformity assessment community can be requested to join in order to provide insights from practitioners, auditors, and experts in the field.

Discussion. In this supportive/advisory role towards partners and other companies, the NCSC can make use of its network of partners to provide workshops and run awareness campaigns. A possible difficulty is identified in the lack of specific expertise in relation to the forthcoming CSA schemes and the relative dependence on certification bodies, which not only have extensive expertise in certification and cybersecurity, but also have a commercial interest in widespread adoption of certifications. This can be mitigated however by asking for specific

input from the CABs, while the NCSC maintains control of the workshops. The NCSC can make use of the opportunity the CSA offers with a significant change in the landscape, as identified by several interviewed stakeholders. Another positive aspect is fostering and strengthening the existing fora and collaborations, such as with the DTC and the Digital Trust Community.[248] Role 2 is within the current mandate of the NCSC as regards the vital sectors, even though it should be carefully put forward to avoid any overlapping efforts from the national cybersecurity certification authority.

S	Supportive role
#2	Awareness raising and training
Strengths	• Experience in providing workshops and awareness raising[249] • Within current legal mandate • Use of existing communication channels such as ISACs
Opportunities	• Help current partners • Expand network to new partners and conformity assessment bodies • Learn from information shared by conformity assessment experts
Obstacles/Risks	• To be viewed as promoting certification services (: maintaining control of the content of campaigns/trainings, and a neutral stance is necessary. Talk about both added value and risks) • Certification as such not a core business (: can be mitigated by collaborating with CABs). • Duplication of work, should other agencies in NL decide to do something similar (: coordination/collaboration is necessary)

Table 10: Overview of Role #2 key aspects

Role 3: Provide assistance to the national cybersecurity certification authority in its tasks (supportive/reactive role)

Background. MinEZK will be the competent cybersecurity certification authority, which will delegate the task to the Radiocommunications Agency (AT). Although the AT has a long track record in oversight in the telecommunications market, cybersecurity certification is a relatively new unexplored area for the AT. Besides, CSA certification is also relevant to sectors and application areas in which the AT or other agencies, such as the AIVD, have little experience. The NCSC, due to its strong involvement in incident management, is in the unique position to get valuable information from the field that could also be relevant for certification as it can provide insight in areas or topics for which standards and best practices could be developed, or which deficiencies of a certification scheme exist. It can bring information to the table from all vital sectors (whereas the AT currently only has an overview of the energy and telecom sectors) and more partners. Moreover, the NCSC has a type of relationship with its partners which differs from the supervisory role the AT currently has for energy and telecom, and is expected to have with certification holders. The NCSC, as mentioned before, is perceived as a trusted partner available to assist its partners. Players in the field report that they can share sensitive information about incidents, threats, measures (not) taken with the NCSC without having to fear regulatory interventions or sanctions.

The AT is expected to have both operational and supervisory roles. The operational role includes advising market players on cybersecurity certification. This requires an internal separation of units and people involved with the respective tasks within the AT. Yet, this may not be enough to give companies the confidence to exchange sensitive information with the AT (advisory branch). The market may still perceive an entanglement of

advisory/supervisory tasks. A possible way to mitigate this (perceived) conflict would be to designate NCSC as an information provider for cybersecurity certification while maintaining all supervisory roles at AT.

Possible ways forward. The CSA places particular emphasis on safeguards for the quality and reliability of the certification process. One of those guarantees is monitoring of implementation issues of the schemes. The NCSC could adopt a monitoring support role for the AT obtaining relevant information from NCSC's partners and transforming this into information that enables the AT to act, without disclosing information that may put the sources in further risks. On the basis of monitoring developments on the floor, the NCSC can also detect other cybersecurity issues within the realm of AT oversight, and bring aggregated data to the attention of the AT without potentially affecting the relationship between AT and parties in the field.

Another area where the NCSC can support the AT is by building up further expertise on technologies and their vulnerabilities in the operational domain, that can be consulted by the AT when necessary. This would potentially be more efficient than having each entity develop expertise on specific technologies. This would require making clear arrangements within the various entities involved in cybersecurity (AT, AIVD, MIVD, NCTV, etc.) where technical expertise resides (collaboration instead of pseudo competition).

Moreover, the NCSC can support the AT in its tasks during the evaluation for high-assurance level certifications. Upon request by the AT, the NCSC may provide non-binding advice in specific cases with high-complexity. The NCSC has the expertise to provide such advice, because of its close collaboration with the vital sectors, which equip the NCSC with knowledge not met in other agencies, in such depth at least. The collaboration for a complex assessment could benefit from combined advice of actors such as the NCSC and the AIVD, depending on the scope of assessment.

Furthermore, the NCSC could identify new areas and topics for European Cybersecurity certifications and communicate them to the AT, and in turn to the ECCG, which has the power to request ENISA to prepare candidate schemes. Such information on needs and trends for the development of new certifications would be gathered from NCSC's partners.

Last, Art. 57 CSA provides national certification schemes on topics covered by a European cybersecurity certification scheme cease to produce effects. However, with a few exceptions, certification schemes might have partially overlapping scope with the European ones. This practically means that some knowledgeable and reliable body needs to make such an assessment of the overlapping scopes and the conflicts between national and European schemes. This is not a task necessarily reserved for the national cybersecurity certification authority, and the NCSC could take on this supportive role in collaboration with the AT and conformity assessment experts.

Discussion. The supportive and reactive roles towards the national cybersecurity certification authority are relevant to current activities for the Agency. The AT remains the national cybersecurity certification authority responsible for cyber security certification. The NCSC could facilitate the AT from its operational knowledge regarding cyber incidents and their mitigation as well as with the general cybersecurity knowledge present and being developed at the NCSC. Knowledge of standards, standardisation, conformity assessment and accreditation can help NCSC to provide relevant information to support AT's roles. Another consideration is that the AIVD is put forward by some governmental interviewees as the go-to expert given their current expertise with high assurance security certification. It deserves further exploration whether indeed cybersecurity certification can do entirely without the help of the NCSC, and whether the knowledge of the AIVD on Common Criteria is

sufficiently addressing all the issues pertaining to vital sectors. It should also be noted that other interviewees urged for the Dutch regulator to use its full capacity as a whole and to avoid duplication of work and additional efforts building new capacity in some governmental agencies, which already exist in another.

S/R	Supportive/reactive role				
#3	Provide assistance to the national cybersecurity certification authority (AT)				
Options	Monitoring implementation of European certifications and reporting aggregated data to AT	General consultation role towards AT regarding vital sectors' cybersecurity issues, relevant for CSA certifications at large	Providing non-binding advice to AT during evaluation of high-assurance level certifications	Identification of new areas and topics of certification based on NCSC's partners and communication to AT.	Gap and overlap analysis of national and CSA schemes
Strengths	• Deploying NCSC expert knowledge				
Opportunities	• Help current partners by communicating their certification needs to the AT • Strengthen collaboration with AT • Complement advice of the AIVD on an as-needed basis • Avoid duplication of work of Dutch regulator at large				
Obstacles/ Risks	• Compromise of trust relationship with partners if shared information is not aggregated and anonymised (: anonymisation of input is a necessary condition for this role) • Potentially little experience in gap and overlap analysis in certification				

Table 11: Overview of Role #3 key aspects

Role 4: Provide knowledge and expertise during accreditation of certification bodies (reactive role)

Background. The Cybersecurity Act obliges certification bodies and authorities to obtain accreditation for their CSA certification services. Accreditation will be conducted by the National Accreditation Body in line with the Regulation 765/2008. The RvA works with both internal and external resources for carrying out assessments. The RvA has in-house expertise allowing it to assess whether a conformity assessment body is competent to carry out a specific conformity assessment activity. In-house expertise is not necessarily present with regards to cybersecurity certification specific criteria. In areas that require a high level of expert knowledge, the RvA often collaborates with freelance experts who perform evaluations on its behalf. The decision on granting the accreditation is made by the RvA. NCSC is seen by many as having much in-house cybersecurity expertise. As such, it could play a role as a regular/preferred knowledge provider to the RvA. The added value for NCSC would be to further keep up with the state of the art regarding cybersecurity certification as a result of being involved in accreditation of CSA schemes, which in turn will facilitate NCSC in their information roles outlined above.

Possible way forward. The NCSC could collaborate with the RvA on an as-needed basis by providing experts to assist the RvA in its accreditation assessments. This collaboration should not be confused with the supervisory activity of Art. 58(7)(c) CSA, which provides that the national cybersecurity certification authority has the power to "actively assist and support the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies".

The proposed role concerns assisting the RvA in conducting the assessments on whether a certification body fulfils the requirements, in particular those pertaining to cybersecurity expertise, to receive accreditation. Thus, this is a 'reactive' role, responding to requests of the RvA to the NCSC for lending its expertise, rather than a

proactive supervisory or monitoring role, that is reserved for the AT, as the competent certification authority. A similar practice is currently prescribed in the General Data Protection Regulation. Art. 43(2) of the GDPR provides three possible accreditation models of certification bodies, in which 1. the supervisory authority (Data protection Authority) provides accreditation, 2. The National Accreditation Body provides accreditation in line with ISO/IEC 17065/2012 and the additional data protection requirements established by the Data Protection Authority, or 3. By both the National Accreditation Body and the Data Protection Authority.[250] The last model is a joint accreditation process, by both the NAB and the DPA, whereby the DPA complements the NAB in terms of data protection expertise. In the Netherlands, the RvA is the entity responsible entity for the accreditation, however the AP is also involved in the process.[251]

Discussion. The role of lending expertise to the accreditation procedure conducted by the RvA builds on the accumulated knowledge of the NCSC in cybersecurity. However, the NCSC experts would potentially require additional training with regard to conformity assessment rules and procedures or need to be assisted by an experienced (in conformity assessment) RvA expert. This role does not fall within the current mandate of the NCSC, although, strictly speaking, it is not prohibited.

Furthermore, this is a role that cannot be covered by the AT, which has a supervisory role in relation to accreditation. A possible difficulty could arise if public bodies in the Netherlands start offering services for high-assurance level certifications in the future, as foreseen in the CSA.[252] In that case, the NCSC would have to assess the cybersecurity level of a public authority. Nevertheless, the RvA would be the end decision maker in granting the accreditation, which is not less of a problem, since the RvA is an independent government agency, answering to the Ministry of Economic Affairs and Climate Policy.[253] Another issue to be considered is the fact that this role could undermine or conflict with the supportive roles, either directly –due to requirements of independence of the evaluators– or indirectly, by impacting the trust collaborative relationship between the NCSC and its partners. A last consideration is a client relationship with CABs and a competitive relationship with other freelance assessors, which however can be avoided by establishing a framework of collaboration with the RvA, addressing such issues. Despite the above obstacles, the added value of such as role in contributing to proper assessments, is a plus for the reliability of the accredited certification bodies, and in turn certifications.

R	Reactive
#4	Provide expertise during accreditation of certification bodies
Strengths	• Utilising existing expert knowledge in cybersecurity
Opportunities	• Growing in new fields and establishing new partnerships: Raad voor Accreditatie • Indirectly helping AT by providing reliable assessments (*could be particularly useful for CABs intending to offer services for high-assurance ICT products/processes/services)

Obstacles/Risks	• Not clearly within current mandate • Might be conflicting with recommended advisory roles #1 and #2: acting as partner and participating in the CABs accreditation assessment. • Competitive relationship with other freelance assessors or consultancies (: can be avoided by taking on a specific type of assessments e.g. high assurance, and low/medium can be left for other assessors) • Client relationship with CABs (: can be avoided by establishing a general collaboration framework with the RvA, following the example of the GDPR/AVG accreditation model and the collaboration between AP and RvA). • Participation in such assessments not core business for NCSC, perhaps lacking experience (: joint assessments with RvA auditors experienced in conformity assessment – complementary knowledge)

Table 12: Overview of Role #4 key aspects

Role 5: Contribution to development of standards and certifications (reactive role)

Background. Monitoring developments and sharing knowledge may contribute to taking a more active form than the previous proposed options. That is by actively contributing to the development of standards and certification schemes. Both in terms of standardisation and certification, the expertise of the NCSC-NL is valuable for national, European and international activities. Contributing to the drafting or offering expert advice and feedback, may increase the quality of standards and schemes, offer inside information to the NCSC about the developments, and strengthen its profile to a broader audience.

Possible ways forward.

A. Participate in a structured manner in standards development. As provided by the Dutch standardisation institute, NEN, standardisation committee members have a facilitating role, being the "ambassadors" of the Dutch stakeholders to the European and international committees. The NCSC already participates in the relevant Information Security, Cybersecurity and Privacy committee of NEN. The participation however could be done in a more systematic manner, with an agenda to

1. identify new topics/elements for standardisation based on mapping the needs of NCSC's partners and
2. communicate those by contributing to the existing activities of CEN-CLC/JTC 13 "Cybersecurity and Data Protection" and ISO ISO/IEC JTC 1/SC 27 "Information security, cybersecurity and privacy protection."

The CEN-CLC/JTC 13 is specifically working on standards and other documents in support of the EU Cybersecurity Act, thus the NCSC could directly influence the standardisation developments in relation to the CSA.

B. Participate in European cybersecurity certifications development. ENISA, in its task to prepare candidate certification schemes, is assisted by ad hoc groups. The NCSC could take on a role of participating in those groups, where a topic is of particular interest or potential impact for the Dutch stakeholders. An example of a candidate scheme with expected significant impact is the EU Common Criteria. In the ad hoc working group, there is a diversity of stakeholders participating, such as conformity assessment bodies (including a Dutch lab), security authorities, and industry representatives from critical sectors and others.[254] This role is not preserved for the national competent authorities, such as the AT, which participates in the preparation of the schemes via the European Cybersecurity Certification Group (ECCG), tasked to

provide advice and feedback throughout the preparation process.

Discussion. The roles proposed in this section are building on the existing practice of the NCSC. They have a strong cross-border nature, as the NCSC is the vehicle to put forward the interests and needs of the Dutch stakeholders and influence developments, which will have an impact on the Dutch market. An eventual step before making the most of this role is an inventory of the skills and expertise currently present in the NCSC. It might be necessary for the NCSC to strengthen its knowledge in relation to certain topics, such as gaining more expertise in SCADA or other sector-specific systems. In this proposed role, there is no foreseen conflict with AT's activities, but coordination might be useful to ensure a common front of Dutch stakeholder needs towards the European and international counterparts.

R	Reactive
#5	Contribute to standards development and certification
Options	Structured participation in standards development Participation in ad hoc working groups of ENISA
Strengths	• Growing on an already established function (participation at NEN committees and ESOs, ISO/IEC committees via NEN)
Opportunities	• Expand network of collaborators and partners • Expand expertise in certification by participating in the making of candidate schemes and learning from ENISA and other participants • Be informed about the latest developments • Direct contribution to the developments • Help partners' needs to be heard at the various standardisation and certification organisations/groups.
Obstacles/Risks	• Limited knowledge in relation to specific technologies • Lack of common line with AT (: no conflicting roles with AT, but coordination for a common Dutch policy front might be good to have)

Table 13: Overview of Role #5 key aspects

Role 6: Develop own scheme (proactive role)

Background. While the development of CSA cybersecurity certification schemes is entrusted to ENISA, cybersecurity certification and seals may also be developed at national level, as long as they do not overlap with the European ones. In fact, several National Cybersecurity Agencies in other Member States (and the UK) are involved in certification at large or have their own standards and seals. The interviews and the research for the study revealed that such an approach would be appreciated by some of the stakeholders. Other stakeholders find no particular value or reason for such a role either speaking from a governmental point of view or from an industry perspective, since there are already several options available in the market.

Possible ways forward.

A. Develop NCSC "trusted party" scheme. Information sharing among stakeholders requires a level of trust. While there are already mechanisms in place to ensure that information is shared among trusted parties within ISACs (such as operating in "inner circles" or with Traffic Light Protocol), enlarging the collaboration and information platform would necessitate more advanced ways in building trust. A possible solution for the NCSC is to create

its own trusted party scheme to offer guarantees of expertise, confidentiality, and added value to the group of partners. A relevant option would be assurance of service providers in cybersecurity.

- The NCSC-UK for example provides certification of professional NCSC Assured Service Providers. All the certified providers are included in a pool of expert consultancies, which meet the quality criteria of the NCSC-UK.[255] The NCSC-UK also provides other certifications: Cyber Essentials,[256] Certified Assisted Products, Cyber Security Professionals, Certified Training and Certified Degrees, Penetration Testing, Commercial Product Assurance, Assured Services, and Cyber Incident Response.[257]
- The NCSC-UK has been working with the so-called Fusion Cells, which are cyber-attack monitoring operations rooms, with participation of industry (cross-sector) and government.

B. Develop own cybersecurity label. A proactive potential role for the NCSC is to develop its own cybersecurity label for products and systems. This could entail either the development of a homegrown 'standard' or building on a combination of existing standards. The NCSC-NL cybersecurity label would be voluntary, and the purpose would be to help its partners navigate through the jungle of standards, and to support the supply chain security, and international collaborations.

- An example of such a scheme developed by another NCSC is the German Bundesamt für Sicherheit in der Informationstechnik (BSI) certification which assesses the security statements/claims of vendors for products.[258] This meta-scheme is lighter than regular conformity assessment activities, and offers tangible benefits to the users of certified products.[259]

The NCSC would not need to administer the scheme, as such a role can be played by other independent organisations with expertise in the field, such as NEN.

Discussion. The options outlined in this section require moderate to substantial effort to materialise, in addition to a potential update of the mandate of the NCSC. Furthermore, as this is not NCSC's core expertise it would need to obtain the expertise and resources, especially in the case of its own cybersecurity label, and ensure that it has a clear place in the market among the multitude of other certifications.

In adopting such a role, the NCSC would also need to ensure that its statutory role stemming from the Wbni and the Bbni, would be separated from the certification services, to avoid conflicts of interest and compromise of independence. Despite these obstacles, this proactive role could bring added value to both the profile and capacity of the NCSC, its partners, and cybersecurity in general, since in the first option information sharing would be done among verified trusted parties, and in the second option, the NCSC label would guarantee quality assurance and rigorous assessment. Especially, in the case of a trusted party scheme, trusted groups could grow further than information sharing and analysis, in working together in teams doing tests similar to the threat intelligence-based ethical red teaming (TIBER), established in the banking sector.[260] In addition, the NCSC-NL could exchange best practices with its counterparts in other countries, which are active in certification (UK, France, Germany, Italy, and others).

P	Proactive	
#6	Develop own scheme	
Options	Develop NCSC "trusted party" scheme	Develop own cybersecurity label

Strengths	• Utilising existing cybersecurity expertise • Addressing an existing target audience (partners and collaborators)
Opportunities	• Helping fostering trust among partners • Facilitating the growth of trusted partners (see Role #1) • Boost information and knowledge exchange among a larger group of entities • Strengthening relationships with other cybersecurity agencies with similar activity such as the UK and DE
Obstacles/Risks	• Outside the current mandate • Function creep in option nr. 2 (can be mitigated with functions/departments separation within the NCSC, see also ISO/IEC 17065) • Possibly limited knowledge in drafting schemes (could be assisted by CABs, or by participating in the ad hoc WG of ENISA, Role #5) • Lack of experience in operating schemes (independent entity such as NEN could take over this role) • Risk of client relationship if fees are charged (see risk mitigation measures in other agencies)

Table 14: Overview of Role #6 key aspects

Last but not least, several of the proposed roles position the NCSC as a knowledge centre with an established network of trusted partners within the vital and other sectors. Strengthening the capacity and profile of the NCSC in this area is useful for future developments in the field of cybersecurity. An example is the European Commission Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, which recently received the green light from the Council for new negotiations with the European Parliament.[261] The NCSC could take on the role of the National Coordination Centre, which according to the Commission proposal would need to 1. "possess or have direct access to technological expertise in cybersecurity" and 2. "be in a position to effectively engage and coordinate with industry, the public sector and the research community."[262]

8 Conclusions

The aim of this Report was to examine whether and how the Dutch cybersecurity certification landscape has started to respond to the EU Cybersecurity Act and whether the needs of stakeholders point at the direction of NCSC in having a role in the evolving landscape (and which roles those would be).

There are several developments to be expected in the forthcoming year. Especially at the legislative level, the Dutch law adapting the national legislation to the CSA, which is currently being drafted, is expected to be voted and adopted. The law will designate the Radiocommunications Agency (EZK) as the national cybersecurity certification authority in the Netherlands. Second, the first European cybersecurity certification schemes which are now being developed by ENISA will be adopted by the European Commission. Thus, the reaction of the market currently can only be measured on the basis of intentions and interest of the stakeholders. An indicator of interest in engaging with the new cybersecurity schemes is the intention to apply for accreditation and offer services based on those future schemes.

Despite this evolving setting, there are several key findings from both the desktop research and the expert interviews. Those findings informed the section sketching the potential role of the NCSC in the cybersecurity certification landscape in the Netherlands, together with the assessment of NCSC's current mandate and framework of operation.

A first issue is the fragmentation of the regulatory landscape and the multitude of governmental agencies dealing with some aspect of cybersecurity, including standardisation and conformity assessment. A centralised approach has been put forward by interviewees, who find value having to deal with a single regulator. The complexity of the landscape often leads to confusion (who is the competent authority? Who has the right expertise for X issue? To which authority do I report a breach?) and obscurity, which brings along risks and in any case, does not foster a healthy relationship between regulator and regulated entities. Apart from the governmental actors, Public Private Partnerships are also many, often overlapping. While PPPs offer excellent opportunities for collaboration and information sharing among their participants, experts report that sometimes those are inactive and might not work as initially planned. Besides, regulatees spend considerable resources on all those different initiatives.

Another issue is the lack of awareness regarding the added value of independent assessments and certification. While industry in the critical infrastructure is made aware of the importance of cybersecurity certification, including through the duty of care imposed by the Wbni, smaller organisations in other sectors, are not familiar with certification. Even in the critical infrastructure, organisations often opt for second party assessments instead of certifications, since smaller companies in the supply chain cannot afford certification. Moreover, unless certification becomes mandatory, certain stakeholders tend to maintain a hesitant stance due to its high costs as opposed to clear added value. This issue is related to the uneven distribution of cybersecurity costs in general, as identified in the Cybersecurity Assessment (2019), and the lack of incentives to re-adjust the cost-benefit ratio.

The EU Cybersecurity Act is expected to stir the Dutch cybersecurity certification landscape. Much will depend on the scope of the European certifications, which will determine which sectors will be urged or possibly required by law to undertake a certification process. Many conformity assessment bodies, established in the Netherlands, plan to seize the new opportunity and get accredited in order to provide services for the new certifications. The success of the voluntary certifications is also expected to depend on the added value it brings to the certification

holder. Compliance with legal obligations, participation in procurements, enhancement of trust and reliability in business to business and business to consumer relationships are drivers that urge companies to pursue certifications.

In general, the interviewed experts for this study consider the NCSC a respected agency, concentrating unique expertise in cybersecurity and playing an active role in emergency response, but also knowledge sharing. Nonetheless, the mandate of NCSC is not always clear, especially to non-partner organisations, such as conformity assessment bodies. In addition, it is clear that the Netherlands is and should continue being an active actor in the European arena, both in terms of standardisation and certification.

In this landscape, the NCSC has several options to move forward, ranging from supportive, reactive to proactive roles. Facilitating knowledge sharing on cybersecurity certifications via national ISACs, or other informal collaborations, raising awareness and conducting trainings, expanding voluntary collaborations with certification bodies and other stakeholders are in general roles within the current mandate of the NCSC, with strong supportive character. NCSC could also explore the option of providing substantial assistance to the national cybersecurity certification authority in providing advice during the assessments of high assurance certifications, or providing aggregated data on deficiencies in the implementation of schemes. Alternatively, the NCSC could lend its expertise to the National Accreditation Body to conduct assessments of certification bodies. Further, continuing and systematising the current work of the NCSC in standardisation, could be valued by its partners, as promoting their interests at national, European, and international fora. Last, following the example of the National Cyber Security Centres of other countries, the NCSC-NL could develop its own national scheme and label, in areas not covered by the European cybersecurity certifications.

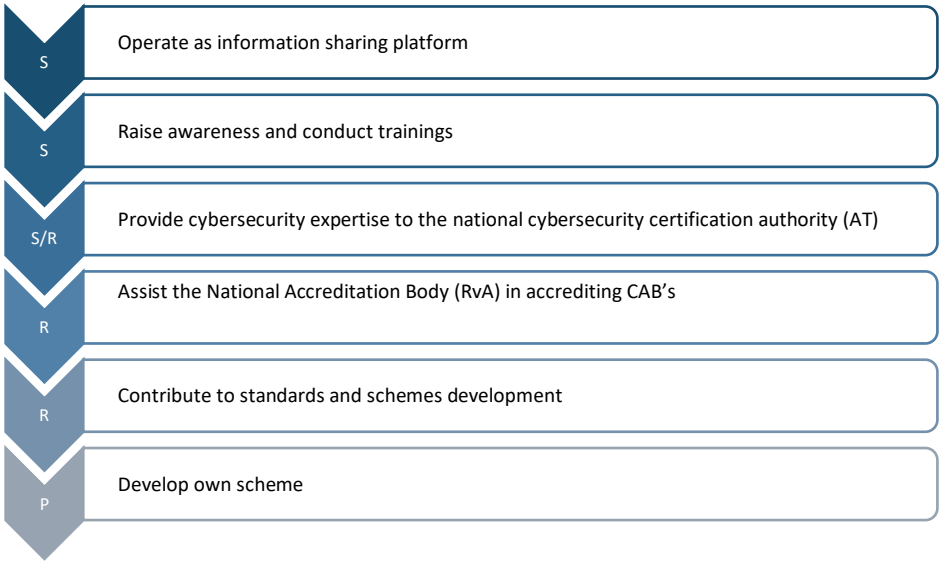


Figure 6: Overview of potential new/extended roles for NCSC

All those options, bring forward two main elements of the NCSC: the trusted partnerships and deep expert knowledge in the field. The study showed that there are issues to be considered when adopting some of those options such as maintaining the trust relationship with its partners, and expanding its legal mandate. On top of any future role of the NCSC in the certification landscape in the Netherlands, the Agency should keep an eye for

other forthcoming related developments, which may strengthen its mandate, such as the ongoing revision of the NIS Directive.

Bibliography

Adams Samantha, Brokx Marlou, Dalla Corte Lorenzo., Galič Maša, Kala Kaspar, Koops J. Bert, Leenes Ronald, Schellekens, Silva E. Karine, Skorvánek Ivan. "The Governance of Cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK, Tilburg University, (2015).

Arampatzis, Anastasios. "What Is the ISA/IEC 62443 Framework?", The State of Security, 2019, https://www.tripwire.com/state-of-security/regulatory-compliance/isa-iec-62443-framework/

Autoriteit Consument & Markt. "Incentive Regulation of the Gas and Electricity Networks in the Netherlands", General Information about the method of regulation of the system operators of natural gas and electricity in the Netherlands by the Netherlands Authority for Consumers and Markets, May 2017. https://www.acm.nl/sites/default/files/old_publication/publicaties/17231_incentive-regulation-of-the-gas-and-elektricity-networks-in-the-netherlands-2017-05-17.pdf

Besluit van de Minister van Justitie en Veiligheid 2503016/19/DP&O. Houdende Wijziging Van het Organisatiebesluit Ministerie van Justitie en Veiligheid in verband met de verwerking van sturingsafspraken, reorganisaties en enkele correcties', Staatscourant 2019, 23817, published on 01-05-2019

Besluit van 4 december 2017 tot aanwijzing van aanbiedersm proucten en diensten ten aazien waarvan een plicht geldt om ernstige ICT-incidenten te melden – Besluit meldplich cybersecurity

Blot, Philippe. "Insight into the First Steps of the Cybersecurity Act Reality" Presentation at the ETSI Security Week, 10 June 2020.

Centraal Bureau voor de Statistiek. "Cybersecuritymonitor 2019", 2019 https://www.cbs.nl/nl-nl/publicatie/2019/37/cybersecuritymonitor-2019

Cole Mark D., Smitz, Sandra. "The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape." University of Luxembourg Law Working Paper No. 2019-017 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3512093

Commission Implementing Decision M/536 on a standardisation request to the European Committee for Electrotechnical Standardisation and to the European Telecommunications Standards Institute as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council 5376 final of 4.8.2015 (2015)

Coördinatiebesluit Decree of 20 January 2011, regulating the powers with regard to the arrangement of the organization and management of the civil service (Coordination decision organization and management civil service 2011).

Craigen, Dan, Diakun-Thibaul, Nadi and Purse Randy. "Defining Cybersecurity," Technology Innovation Management Review (2014):13-21.

Criminal Code of Procedure (CCP). Law of 15 January 2021 concerning rules of criminal procedure (Code of Criminal Procedure).

Custers, Bart. "Nieuwe Online Opsporingsbevoegdheden en het Recht op Privacy – Een analyse van Computercriminaltiteit III", eLaw Working Paper Series no. 2018/004, (2019)

De Hert, Paul, Papakonstantinou, Vagelis, and Kamara, Irene. "The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection" Computer Law & Security Review, (2016): 16-30.

Directive 2014/30/EU, as amended by Regulation 2018/1139 (EU) of the European Parliament and the Council

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Dutch Cybersecurity Agenda. "A cyber secure Netherlands" (2018), https://english.ncsc.nl/topics/national-cybersecurity agenda/documents/publications/2019/juni/01/national-cyber-security-agenda

Dutch Parliamentary Chamber. Parliamentary letter on cyber-attack Not-Petya (2017), https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2017Z12348&did=2017D25970.

ECORYS. "Security Regulation, Conformity Assessment & Certification Final Report – Volume I: Main Report" Brussels, October 2011.

ENISA. "Definition of Cybersecurity – Gaps and Overlaps in Standardization", v.1 (2015).

ENISA. "Overview of cybersecurity and related terminology" v.1 (2017), https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology.

ENISA. "Standards supporting certification, Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes", December (2019).

ETSI. "Final draft ETSI EN 303 645 v2.1.0 (2020-04), CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements" REN/CYBER-0048.

European Commission. Communication 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM 410 final, (2016)

European Commission. Cybersecurity in the European Digital Single Market (Scientific Opinion No. 2, 2017), https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf.

European Union Agency for Cybersecurity. "Handbook on Security of Personal Data Processing", January 2018.

Fovino, Igor N., Neisse, Ricardo; Hernandez Ramos, J. L, Polemi, Nineta; Ruzzante, Gian-Luigi, Figwer, Malgorzata, and Lazari, Alessandro. "A Proposal for a European Cybersecurity Taxonomy." Luxembourg: Publications Office of the European Union, (2019), ISBN 978-92-76-11603-5 https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf.

Ganji, Daniel, Kalloniatis, Christos, Mouratidis Haralambos, H, and Gheytassi, S. Malekshahi. Approaches to Develop and Implement ISO/IEC 27001 Standard-Information Security Management Systems: A Systematic Literature Review. International Journal on Advances in Software Volume 12, Number 3 & 4, (2019), 228 – 238.

Grondwet Constitution of the Kingdom of the Netherlands of August 24, 1815.

Kamara, Irene., Leenes, Ronald., Lachaud, E., Stuurman, Kees., Van Lieshout, Marc., & Bodea, Gabriela. Data Protection Certification Mechanisms: Study on Articles 42 and 43 of the Regulation (EU) 2016/679. (1 ed.) Brussels: European Commission - DG Justice & Consumers, 2019 https://doi.org/10.2838/115106

Kamara, Irene. "Misaligned Union laws? A Comparative Analysis of Certification in the Cybersecurity Act and the General Data Protection Regulation", Hallinan D., Leenes, R., De Hert P,(eds.) Privacy and Data Protection: Artificial Intelligence, Hart Publishing, [forthcoming 2020]

KPMG. "Export Opportunities of the Dutch ICT Sector to Germany Report, (2017).

Lachaud, Eric. ISO/IEC 27701: Threats and opportunities for GDPR certification, European Data Protection Law Review, 6(2), (2020): 194-210.

Leteinturier, Aurelien; Larrumbide Borja; Tuinsma Bert; Doubrava Clemens; Catteddu Daniele; Graux Hans; Orue-Echevarria Leire; Niessen Thomas; Vreeburg Tom; Ochs William. « Recommendations for the Implementation of the CSP Certification Scheme", CSPCERT WG, 2019.

Law of 2 July 1998, containing rules concerning the production, transport and supply of electricity (Electricity Act 1998).

Law of 22 June 2000, containing rules concerning the transport and supply of gas (Gas Act).

Law of 17 June 2013, containing rules regarding the supply of heat to consumers (Heat Act).

Law of 23 November 2006 amending the Electricity Act of 1998 and the Gas Act in connection with further rules regarding independent grid management.

Mandaatbesluit Ministerie van Justitie en Veiligheid Decree of the Minister of Justice and Security of 29 October 2018, no. 2388102/18 / DP & O, granting a mandate, power of attorney and authorization (Mandate Decree Ministry of Justice and Security)

Ministry of Economic affairs and Climate Policy. "CSIRT voor Digitale Dienstverleners: Directoraat-Generaal Bedrijfsleven en Innovatie | Directie Digitale Economie" (2019), https://csirtdsp.nl/sites/default/files/2019-03/20190318_CSIRT%20DSP_RFC2350v1.1.pdf.

Ministerie van Economische Zaken en Klimaat; Ministerie van Justitie. "Roadmap Digitaal Veilige Hard- en Software" Den Haag, April (2018)

Microsoft. Security Intelligence Report Microsoft, Vol. 24, January – December 2018), https://www.microsoft.com/security/blog/2019/02/28/microsoft-security-intelligence-report-volume-24-is-now-available/.

Nationaal Coordinator Terroorismebestriijding en Veiligheid (NCTV). "National Crisisplan Digitaal." (2020)

National Cybersecurity Agenda. "A cyber secure Netherlands" (2018) https://english.ncsc.nl/topics/national-cybersecurity-agenda/documents/publications/2019/juni/01/national-cyber-security-agenda.

NEN. Commissieplan: Norm(sub)commissie 381027, Informatiebeveiliging, Cyber security en Privacy (2017), https://www.nen.nl/Home_EN/Informatiebeveiliging-Cyber-security-en-Privacy.htm.

NIST SP 800-37 Rev. 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy" (2018), https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

NIS Cooperation Group. "Sectorial Implementation of the NIS Directive in the Energy Sector" Report - CG Publication 03/2019 (2019).

ISO/IEC 17000:2004 (en) Conformity assessment — Vocabulary and general principles«, ISO, https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-1:v1:en.

ITU, Overview of Cybersecurity: Recommendation ITU-T X.1205, Geneva: International Telecommunication Union, (2009). http://www.itu.int/rec/T-REC-X.1205-200804-I/en.

Organisatiebesluit Decree of the Minister of Justice and Security of 28 November 2017, reference DP & O / 17/2150354, establishing the organization of the Ministry of Justice and Security (Organization Decree Ministry of Justice and Security).

Pieters, Janene. "Maastricht University Paid €250K to ransomware hackers: report," NLTimes, January 24 (2020), https://nltimes.nl/2020/01/24/maastricht-univ-paid-eu250k-ransomware-hackers-report.

Regeling Agentschappen Regulation of the Minister of Finance of 21 November 2017, containing rules on the establishment, organization and management of the agencies (Agencies Regulation).

Regulation (EC) No 714/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity and repealing Regulation (EC) No 1228/2003 and Regulation (EC) No 715/2009 of the European Parliament and of the Council of 13 July

2009 on conditions for access to the natural gas transmission networks and repealing Regulation (EC) No 1775/2005.

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)

Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems COM/2019/546 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546 (accessed 10 February 2020).

Rijksoverheid, Regeerakkoord: 'Vertrouwen in de Toekomst' (2017).

Rijksoverheid. Nederlandse Cybersecurity Agenda – Nederland Digitaal Veilig (2018), https://www.rijksoverheid.nl/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig.

Telecommunicatiewet Law of 19 October 1998 concerning rules regarding telecommunication (Telecommunication Act)

Tweede Kamer der Staten-Generaal, "Reactie inzake cyberaanval met ransomware en voortgang moties uit Wannacry-debat", 487 (2017).

Vetillard, Eric. "The Cloud Services Candidate Scheme", Presentation at ETSI Security Week, 11 June 2020.

Law of 17 October 2018, containing rules for the implementation of Directive (EU) 2016/1148 (Network and Information Systems Security Act).

World Today, "Data breach in RIVM infection radar, user data available | now," *World Today,* June 6, 2020, https://world-today-news.com/data-breach-in-rivm-infection-radar-user-data-available-now/

ANNEX 1: Accredited conformity assessment bodies in the Netherlands (cybersecurity)

The following Table provides an overview of conformity assessment bodies accredited by the National Accreditation Body in the field of cybersecurity.[263]

Name	Type CAB	RvA Discipline	Relevant standards	Certification scheme
TÜV Rheinland Nederland B.V.	CB	Product certification	ISO/IEC 15408-1, -2, -3, Common Criteria for Information Technology Security Evaluation (CC), and ISO/IEC 18045, Common Criteria Evaluation	Netherlands Scheme for Certification in the area of IT security [NSCIB]
DEKRA Certification B.V.	CB	Management systems	ISO/IEC 27001, ISO/IEC 20000-1, NEN 7510 Medical information technology – Information security in healthcare	Information Security Management Systems Accreditation granted in accordance with ISO/IEC 27006, Certification of Information Technology Service Management Systems, Accreditation granted in accordance with ISO/IEC 20000-6, NTA 7515:2016 Conformity assessment - Requirements for bodies providing audits for certification of information security management systems in healthcare
Kiwa Nederland B.V.	CB	Management systems	ISO/IEC 27001	Information Security Management Systems Accreditation granted in accordance with ISO/IC 27006
TÜV Nederland QA B.V.	CB	Management systems	ISO/IEC 27001	Information Security Management Systems Accreditation granted in accordance with ISO/IEC 27006
BSI Group The Netherlands B.V.	CB	Management systems	ISO/IEC 27001	Information Security Management Systems Accreditation granted in accordance with ISO/IEC 27006
Nederlands Certificatie Instituut B.V.	CB	Management systems	ISO/IEC 27001	Information Security Management Systems Accreditation granted in accordance with ISO/IEC 27006
PricewaterhouseCoopers Certification B.V.	CB	Management systems	ISO/IEC 27001	Information Security Management Systems Accreditation granted in accordance with ISO/IEC 27006

Brightsight B.V. IT Security Evaluation Facility	Lab	Test lab	Common Criteria v3.1 - NEN-ISO/IEC 15408-1, -2, -3 - Common Evaluation Methodology v3.1 - NEN-ISO/IEC 18045 For EAL1-EAL7, ALC_FLR.3, ASE_TSS.2	Unknown (type of activity: evaluation of IT-security products
Riscure B.V. Security Lab	Lab	Test lab	Common Criteria v3.1 - NEN-ISO/IEC 15408-1, -2, -3 - Common Evaluation Methodology v3.1 - NEN-ISO/IEC 18045 For EAL1-EAL7, ALC_FLR.3, ASE_TSS.2	Unknown (type of activity: evaluation of IT-security products
TrustCB B.V.		Product certification	ISO/IEC 15408-1, -2, -3, Common Criteria for Information Technology Security Evaluation (CC), and ISO/IEC 18045, Common Criteria Evaluation Methodology for Information Security Evaluation (CEM)	MIFARE Security Certification Scheme - type certification (testing)
Ernst & Young Certify Point B.V.	CB	Management systems	ISO/IEC 27001, ISO 20000-1	Information Security Management Systems Accreditation granted in accordance with ISO/IEC 27006, Certification of Information Technology Service Management Systems, Accreditation granted in accordance with ISO/IEC 20000-6
Brand Compliance B.V.	CB	Management systems	ISO/IEC 27001	Information Security Management Systems Accreditation granted in accordance with ISO/IEC 27006
Duijnborgh Certification B.V.	CB	Management systems	ISO/IEC 27001	Information Security Management Systems Accreditation granted in accordance with ISO/IEC 27006

Digitrust B.V.	CB	Management systems	ISO/IEC 27001, NEN 7510-1 Medical information technology – Information security in healthcare	Information Security Management Systems Accreditation granted in accordance with ISO/IEC 27006, NCS 7510: Conformity assessment - Requirements for bodies providing audits for certification of information security management systems in healthcare for Cluster B: - Managers of personal health information, other than healthcare institutions, NCS 7510: Conformity assessment - Requirements for bodies providing audits for certification of information security management systems in healthcare for Cluster Z: - Healthcare institutions
DNV GL Business Assurance B.V.	CB	Management systems	NEN 7510-1 Medical information technology – Information security in healthcare	NTA 7515 Conformity Assessment - Requirements for Institutions conducting Audits for perform certification of information security management systems in healthcare Accreditation is provided under NTA 7515 and addendum to NTA 7515

ANNEX 2: Interviewed individuals and organisations

	Expert	Organisation
	Government	
1.	Warna Munzebrock, Coordinating senior advisor, Supervision Policy and Sanctions Department	Agentschap Telecom
2.	Rob Huisman, expert	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Ministry of Interior and Kingdom Relations)
3.	anonymous	Ministerie van Economische Zaken en Klimaat (EZK) (Ministry of Economic Affairs and Climate)
4.	anonymous	Ministerie van Economische Zaken en Klimaat (EZK) (Ministry of Economic Affairs and Climate)
5.	anonymous	NCSC
6.	anonymous	NCSC
7.	Matthijs Balder, Senior Policy Officer	NCTV
	Conformity Assessment Bodies	
8.	anonymous, Service Manager, cybersecurity expert	DEKRA Certification B.V.
9.	Vincent Roes, Head of Strategic Development, Vice-President Service Division Product Testing	DEKRA Certification B.V.
10.	anonymous	TÜV Nederland
11.	Remco Kruit, Local Business Field Manager Systems	TÜV Rheinland Nederland
12.	Frank Groenewegen, Chief Security Expert	FOX IT
13.	anonymous	FOX IT
	Energy sector	
14.	Machiel Bolhuis, Adviseur Regulatory Affairs - databeleid	ENECO
15.	Justin Broeders, Manager Privacy and Security	ENECO
16.	Anne Spoelstra, CISO	ENECO
17.	anonymous, Group Information Security Officer	ENEXIS

18.	Donald Kreiken, European Energy Regulation Advisor	TENNET
19.	Ron Wibbelink, Manager Team Corporate Security	TENNET
20.	Johan de Wit, Technical Officer Enterprise Security	SIEMENS Smart Infrastructure
21.	Ton Mes, Product & Solution Security Officer	SIEMENS Smart Infrastructure
	Banking sector	
22.	Hans van Loon, Advisor Cybersecurity	Dutch Bank Association (Nederlandse Vereniging van Banken (NVB))
23	Remco Ruiter, Liaison officer	Dutch Payments Association (Betaalvereniging Nederland
24.	anonymous	Rabobank
	Standardisation organisation	
25.	Tom Hoogendijk, Consultant ICT standardisation	Dutch Standardisation Institute NEN
26.	Harmen Willemse, Programma Manager Schemabeheer	Dutch Standardisation Institute NEN

ANNEX 3: Interview Guidelines

Interview on cybersecurity certification in NL

Background:
This interview is part of the project of the Tilburg Institute for Law, Technology, and Society on cybersecurity certification, commissioned by the NCTV/NCSC. The aim of the project is threefold: 1. Identify the drivers/trends/and needs of stakeholders in the Netherlands with regard to cybersecurity, and cybersecurity certification in specific. 2. To identify the impact of the Cybersecurity Act and the EU developments on cybersecurity certification. 3. And sketch the role of the NCSC in this landscape for example towards its regulatees (e.g. operators of essential services in different sectors) and the other authorities and agencies.

Questions:

A. General questions about the company

- What is the nature (public/private) of your organization?
- How many employees does your organisation have?
- What is the core business/services that your organisation offers?
- In which countries is your organisation operating? If more than one, are the headquarters in NL?
- To what type of clients does your organisation offer services? Any specialization/focus on operators of essential services? Eg. Energy and banking sectors., SMEs?
- What kind of activities is your organisation deploying in the field of cybersecurity? Why are you interested in cybersecurity?
- Since when is your organisation active in the field of cybersecurity certification?

B. Needs – Trends – Drivers of cybersecurity certification in NL (and EU)

- Which cybersecurity or information security national/European/international standards do you certify?
- Are those product/systems/services/persons standards?
- Which are the most commonly adopted cybersecurity or information security standards in energy and the banking sector?
- What are your views regarding the value/significance of cybersecurity certification?
- What do you see as main challenges/obstacles when it comes down to obtaining, maintaining and using certificates?
    - Is cost an issue? What influences the costs of certification? Name some factors.
- Which are the main drivers for a company in NL to obtain certification in cybersecurity in your view?

- Which certifications in your view will be attractive for companies in the future and why?
  - Generic/sector specific?
  - In which topics/areas?
  - ICT products? systems? services? processes? persons/ skills?
- What do you think of mandatory cybersecurity certification? (=imposed by a national or Union law)? Which are the benefits and drawbacks in your view?
- Which are the main drivers for a company in NL to obtain certification in cybersecurity in your view?
- Which certifications in your view will be attractive for companies in the future and why?
  - Generic/sector specific?
  - In which topics/areas?
  - ICT products? systems? services? processes? persons/ skills?
- What do you think of mandatory cybersecurity certification? (=imposed by a national or Union law)? Which are the benefits and drawbacks in your view?
- In several studies, impartiality and integrity is linked to trust in certification. In the website of your organisation, there is a dedicated page on integrity. Would you like to talk more about this?

C. Impact of CSA and EU developments on cybersecurity certification

- As regards regulatory developments in the field: what are the most important sources of information?
- Do you feel adequately informed about the regulatory developments in the field of cyber security?
- Are you familiar with (the main elements of) the European Cyber security Act?
- What will in your view be the impact of the European Cyber security Act: 1. Overall 2. The (energy) sector, and especially existing certifications in the energy sector?
- Do you have a clear view on the impact the CSA will have for your company (threats, opportunities), especially the common European cybersecurity certifications?
- What do you expect of the market uptake of cybersecurity certification, after the Cybersecurity Act?
- Which sectors will be leading?
- What do you see as main drivers for developing the market for cybersecurity certifications? (reputation, supply chain pressure, compliance, …..?
- Do you see a value in Cybersecurity certifications being European (common across th EU) instead of national? Why or why not?
- Do you plan to be accredited for the CSA sybersecurity schemes? Why? What is the added value on top of what you already provide in the field of cybersecurity?

D. Role of NCSC, and Dutch regulator

- Do you collaborate with the Dutch gov/regulators in cybersecurity (certification) issues? With which agencies?
- Are you aware of the NCSC, their role & powers?
    - Has your organisation ever contacted or cooperated with the NCSC?
    - How would you describe your evaluation of the role and value of the NSCS in the field?
- What do you miss when you evaluate the current role of the NCSC? In other words: which additional advisory/supportive roles/tasks could the NSCS in your view take on to stimulate the developments or improve the quality of current processes in the field? (providing more information, sharing more expertise, contribute more actively in the development of schemes,…….)
- What role do you envisage from the Dutch regulator, and the NCSC in specific, in the future cybersecurity standardisation and certification landscape in NL?

- in their regulatory capacity (making certificates mandatory?)
- in their capacity as leading IT-customer (stimulating)
- in their capacity as caretaker of the economy (stimulating, funding, research, education, ..)
- as source for sharing knowledge
- as source for disseminating information to the market
- otherwise

- What do you think of a national cybersecurity certification scheme developed or handled by the Dutch regulator?
- Do you feel that the needs of the Dutch market in relation to cybersecurity are well represented in the Union? Where should the regulator put more emphasis? What should be corrected?
- Do you have a view/preference on which (types of) government organizations should be involved specifically in cybersecurity certification?

1 Dutch Cybersecurity Agenda, A cyber secure Netherlands (2018), 9, https://english.ncsc.nl/topics/national-cybersecurity-agenda/documents/publications/2019/juni/01/national-cyber-security-agenda.

2 See Dutch Parliamentary Chamber. Parliamentary letter on cyber-attack Not-Petya (2017), https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2017Z12348&did=2017D25970.

3 Microsoft, Security Intelligence Report, (Microsoft, Vol. 24, January – December 2018), https://www.microsoft.com/security/blog/2019/02/28/microsoft-security-intelligence-report-volume-24-is-now-available/.

4 Janene Pieters, "Maastricht University Paid €250K to ransomware hackers: report," NLTimes, January 24, 2020, https://nltimes.nl/2020/01/24/maastricht-univ-paid-eu250k-ransomware-hackers-report.

5 World Today, "Data breach in RIVM infection radar, user data available | now," June 6, 2020, https://world-today-news.com/data-breach-in-rivm-infection-radar-user-data-available-now/.

6 Read for an overview: ENISA, Definition of Cybersecurity – Gaps and overlaps in standardisation, v.1 (2015) p. 20f.

7 ibid.

8 Jacopo Bellasio et al., Developing Cybersecurity Capacity, A proof-of-concept implementation guide (Cambridge & California: Rand Corporation, 2018), 169.

9 NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (2018), https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

10 ITU, Overview of Cybersecurity: Recommendation ITU-T X.1205 (Geneva: International Telecommunication Union, 2009), http://www.itu.int/rec/T-REC-X.1205-200804-I/en.

11 Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, "Defining Cybersecurity," Technology Innovation Management Review (2014): 13.

12 European Commission, Cybersecurity in the European Digital Single Market (Scientific Opinion No. 2, 2017), https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf.

13 A comparative study on the governance of cybersecurity revealed the different approaches in Member States laws: Samantha Adams et al, "The governance of cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK," (2015).

14 Art. 2(1) CSA.

15 Art. 2(a) of Directive 2002/21/EC

16 NIS Directive 1148/2016 Art. 4(1)

17 See Art. 4(2) NIS Directive.

18 Recital 8 CSA.

19 ENISA, *Overview of cybersecurity and related terminology, v.1* (2017), https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology.

20 Igor Nai Fovino et al, *A Proposal for a European Cybersecurity Taxonomy* (Luxembourg: Publications Office of the European Union, 2019), https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf.

21 Directive (EU) 2016/1148

22 Annex II & III NIS Directive.

23 ISO/IEC 17000:2020(en) Conformity assessment — Vocabulary and general principles«, ISO, https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-1:v1:en.

24 For an overview of conformity assessment terminology, See Annex 1: Glossary in Kamara I., Leenes, R. et al. "Data protection certification mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679 : annexes", European Publications Office, 2019, https://op.europa.eu/en/publication-detail/-/publication/5509b099-707a-11e9-9f05-01aa75ed71a1/language-en

25 "CEN/CLC/JTC 13 Scope," CENELEC, https://www.cenelec.eu/dyn/www/f?p=104:7:152596387669701::::FSP_ORG_ID,FSP_LANG_ID:2307986,25.

26 "Over Forum Standaardisatie," Forum Standaardisatie, https://www.forumstandaardisatie.nl/over-ons.

27 "Internet en Beveiliging," Forum Standaardisatie, https://www.forumstandaardisatie.nl/domein/internet-en-beveiliging.

28 "Onze thema's," ECP, https://ecp.nl/themas/.

29 "About ECSO," ECSO, https://ecs-org.eu/about.

30 Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

31 A 2019 European Commission report explains that: "The energy infrastructure is arguably one of the most complex and, at the same time, critical infrastructures that other business sectors depend upon to deliver essential services. Because of this dependency, a potential disruption for a long period can trigger a cascade of effects in other sectors of society." NIS Cooperation Group (2019). In addition, the Dutch Payment Association reports that 9 in 10 bank customers use mobile devices or Internet banking, which makes the availability and security of the payment chains highly significant. See Betaalvereniging Nederland, Factsheet 2019: https://factsheet.betaalvereniging.nl/en/

32 Rijksoverheid, *Nederlandse Cybersecurity Agenda – Nederland Digitaal Veilig* (2018), 9, https://www.rijksoverheid.nl/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig.

33 Ibid, 17.

34 The latter has only been in effect since July 25th 2017, before losing effect on the 9th of November 2018 when the Wbni implemented the European NIS Directive.

35 NCTV, 'Nationaal Crisisplan Digitaal' (2019), 7, https://www.nctv.nl/documenten/publicaties/2020/02/21/nctv-nationaal-crisisplan-digitaal-_-webversie.

36 Wet Beveiliging Netwerk en Informatiesystemen

37 Wet van 17 oktober 2018, houdende regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen) Article 34, https://wetten.overheid.nl/BWBR0041515/2019-01-01; Wet Gegevensbewerking en Meldplicht

38 See the traveaux preparatoires of the Wbni from the Dutch Senate (Eerste Kamer) via https://www.eerstekamer.nl/wetsvoorstel/34883_wet_beveiliging_netwerk_en as well as recitals 31, 43, 44 of the NIS-Directive.

39 Articles. 10 & 11 Wbni.

40 Ministerie van Economische Zaken en Klimaat

41 Articles 4 & 13-15 Wbni; Besluit van 30 oktober 2018 tot aanwijzing vanhet CSIRT voor digitale diensten en tot vaststelling van het tijdstip van inwerkingtreding van de Wet en het Besluit beveiliging netwerk- en informatiesystemen

42 Article 16 Wbni.

43 Article 7 & 8 Wbni.

44 Algemene maatregelen van bestuur.

45 Article 9 Wbni

46 Articles 10 - 15

47 Article 17 – 22 Wbni.

48 Article 23 Wbni.

49 In Dutch; Staatscourant; Article 25; These appointments of officers have happened in the following Ministerial decisions https://wetten.overheid.nl/BWBR0041515/2019-01-01); Besluit Beveiliging Netwerk- en informatiesystemen (https://wetten.overheid.nl/BWBR0041520/2019-01-01); Besluit aanwijzing CSIRT voor digitale diensten Wbni (https://wetten.overheid.nl/BWBR0041536/2019-01-01); Besluit aanwijzing toezichthoudende ambtenaren Wbni (https://wetten.overheid.nl/BWBR0041503/2018-11-09) ; Besluit aanwijzing toezichthoudende ambetenaren Wbni sectoraal(https://wetten.overheid.nl/BWBR0041503/2018-11-09).

50 Articles 4, 27 – 29 Wbni.

51 Besluit Beveiliging Netwerk- en Informatiesystemen.

52 Articles 2-3 Bbni.

53 Articles 4-6 Bbni.

54 Following article 58 (1) of the Cybersecurity Act.

55 Raad voor Accreditatie.

56 Goedkeuringsbesluitmodel ; See article 52 (5) (6) (7) Cybersecurity Act and appendix X for a visualisation of the Goedkeuringsbesluitmodel.

57 See article 49 (7), 54 (1) and 61 (5) of the Cybersecurity Act

58 Algemene Wet Bestuursrecht

59 College voor Beroep voor het Bedrijfsleven

60 Chapters 11 and 11a of the Dutch Telecommunications Act. Law of 19 October 1998 concerning rules regarding telecommunication (Telecommunication Act).

61 Dutch Cybersecurity Agenda, A cyber secure Netherlands, 32.

62 Wet Politiegegevens

63 Wet Justitiële en Strafvorderlijke gegevens

64 Wetboek van Strafrecht, Wvsr

65 Wet Bestrijding Cybercrime (Computercriminaliteit III)

66 Articles 54a, 138ab, 139d, 248a, 248e, 350d Criminal Code (CC).

67 Art. 4 Wbni.

68 Ibid.

69 Ibid.

70 Art. 2-3 Wbni.

71 Ibid.

72 Art. 3 io. 16 Wbni .

73 Besluit van de Minister van Justitie en Veiligheid van 18 april 2019 (kenmerk: 2503016/19/DP&O), houdende wijziging van het Organisatiebesluit Ministerie van Justitie en Veiligheid in verband met de verwerking van sturingsafspraken, reorganisaties en enkele correcties', Staatscourant 2019, 23817, published on 01-05-2019; article 2.

74 Regeling van de Minister van Justitie en Veiligheid van 13 januari 2020, nr. 2775286, houdende aanwijzing van computercrisisteams als bedoeld in de Wet beveiliging netwerk- en informatiesystemen (Regeling aanwijzing computercrisisteams), article 1.

75 Ibid.

76 Ibid.

77 Ibid.

78 The NCTV provides general coordination of threats to the state and public safety. The NCSC as the central coordinator for the response to cybersecurity threats and incidents. The Telecom Agency is the competent authority for oversight and enforcement concerning cybersecurity certification.

79 Tweede Kamer der Staten-Generaal, Kamerstukken 26 643 nr. 668, 18 februari 2020 https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail/2020Z03270/2020D06897.

80 See chapter 2.c.ii and 2.c.iii.

81 Article 1, 3, 7 NIS-Directive.

82 Artikel 63h1 Organisatiebesluit.

83 Organisatiebesluit.

84 Article 63h1 (1) Organisatiebesluit io. Article 3 Coördinatiebesluit and article 44 Grondwet.

85 Article 63h1 (1) Organisatiebesluit.

86 Besluit van de Minister van Justitie en Veiligheid van 18 april 2019 (kenmerk: 2503016/19/DP&O), houdende wijziging van het Organisatiebesluit Ministerie van Justitie en Veiligheid in verband met de verwerking van sturingsafspraken, reorganisaties en enkele correcties', Staatscourant 2019, 23817, published on 01-05-2019; article 2 Mandaatbesluit Ministerie van Justitie en Veiligheid.

87 Ibid; Article 1 (a) io. (n) Regeling Agentschappen.

88 Article 2 (a) io. Article 3 (1) (a) (b) Wbni io. Appendix 1 under 2 of the NIS-Directive io. Article 63h1 (1) (e) Organisatiebesluit.

89 Article 2 (b) io article 3 (3) Wbni io. article 6 Bbni

90 Article 2 (c) Wbni.

91 Article 3 (1) (c) Wbni io. Article 63h1 (1) (a) Organisatiebesluit.

92 Article 3 (1) (d) Wbni io. Article 63h1 (1) (b) Organisatiebesluit.

93 Article 3 (1) (e) Wbni io article 63h1 (1) (c) Organisatiebesluit.

94 Article 3 (2) Wbni io. Article 63h1 (1) (d) Organisatiebesluit.

95 See also "Crisisbeheersing," NCSC, https://www.ncsc.nl/over-ncsc/crisisbeheersing.

96 Article 63h1 (1) (f) Organisatiebesluit

97 The Dutch cybersecurity landscape is discussed infra.

98 See Directive 2014/30/EU, as amended by Regulation 2018/1139 (EU) of the European Parliament and the Council

99 Registreren en vergunning aanvragen radiozendamateurs," Agentschap Telecom, https://www.agentschaptelecom.nl/onderwerpen/radiozendamateurs/registreren-als-radiozendamateur; "Tips voor veilig gebruik slimme apparaten," Agentschap Telecom, https://www.agentschaptelecom.nl/onderwerpen/tips/beveiliging-slimme-apparaten.

100 See article 58 Cybersecurity Act.

101 Article 58 (8) of the Cybersecurity Act.

102 In accordance with article 65 Cybersecurity Act.

103 Algemene Inlichtingen en Veiligheidsdienst.

104 Nationaal Bureau Veiligheidsverbindingen.

105 Nationale Distributie Authoriteit.

106 See official website National Bureau for Connection Security (NBV): https://www.aivd.nl/onderwerpen/informatiebeveiliging/het-nationaal-bureau-voor-verbindingsbeveiliging-nbv

107 Nederlandse Schema voor Certificatie op het gebied van IT-Beveliging.

108 "Internationale taak NBV," AIVD, https://www.aivd.nl/onderwerpen/informatiebeveiliging/het-nationaal-bureau-voor-verbindingsbeveiliging-nbv/internationale-taak-nbv.

109 Militaire Inlichtingen en Veiligheidsdienst (MIVD).

110 See article 20 Wbni.

111 As announced on the DTC's official website: https://www.digitaltrustcenter.nl/nieuws/digital-trust-center-krijgt-groen-licht-voor-definitieve-voortgang.

112 See official website DTC, https://www.digitaltrustcenter.nl/over-hat-digital-trust-center; "Infosheet Veilig Ondernemen," DTC, https://www.digitaltrustcenter.nl/sites/default/files/2019-12/Infographic%20Veilig%20digitaal%20ondernemen.pdf.

113 Tweede Kamer der Staten-Generaal, Kamerstukken 26 643 nr. 668, 18 februari 2020 https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail/2020Z03270/2020D06897.

114 Ibid.

115 National Cyber Security Centre "Benefits from your ISAC. A practical guide" January 2020.

116 https://www.ee-isac.eu/

117 Commission Recommendation of 3.4.2019 on cybersecurity in the energy sector, C(2019)2400 final.

118 More information: https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership

119 See Annex II NIS Directive.

120 Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems COM/2019/546 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546 (accessed 10 February 2020).

121 Mark D. Cole, and Sandra Schmitz. "The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape." University of Luxembourg Law Working Paper 2019-017 (2019).

122 Article 19 NIS Directive.

123 European Commission, Communication 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410 final

124 Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

125 Art. 4 CSA. The status of ENISA has changed from the one of an 'agencies' under the former Regulation to the one of a 'body' under the CSA.

126 Recital 11 CSA.

127 Art. 46 CSA.

128 Recital 75 CSA.

129 This section is based on Irene Kamara, "Misaligned Union laws? A comparative analysis of certification in the Cybersecurity Act and the General Data Protection Regulation", in Privacy and Data Protection: Artificial Intelligence, ed. Dara Hallinan, Ronald Leenes & Paul de Hert (eds), Hart Publishing, [forthcoming].

130 A 'European cybersecurity certification scheme' is defined as "a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes" (Art. 2(9) CSA).

131 Art. 51 (1)(a) CSA.

132 Art. 51 (1)(b) CSA.

133 Art. 51 (1)(c) CSA.

134 Art. 51 (1)(i) CSA.

135 National cybersecurity certification schemes are replaced by a European cybersecurity certification scheme (Rec. 85).

136 Art. 53 CSA.

137 Art. 54 CSA. Those include elements such as the subject matter and scope of the scheme, the type or categories of ICT products, systems, services covered, the purpose of the scheme, references to technical standards or specifications, the possibility for conformity self-assessment, additional accreditation requirements for conformity assessment bodies, specific evaluation criteria, the use of marks and labels, rules for monitoring compliance, conditions for the certificates, and others.

138 Art. 49(4) CSA.

139 Art. 49 (3) CSA.

140 Art. 49 (5) CSA.

141 Art. 56(5) CSA.

142 Art. 58(7)(c) CSA, Recital 102.

143 Art. 58(8)(a) CSA.

144 Art. 58(8)(b) and (d) CSA.

145 Art. 58(7)(d) CSA.

146 Art. 58 (7)(e) and Art. 60(3) CSA.

147 Art. 58(7)(f) CSA.

148 Art. 58(8)(c) CSA.

149 Art. 58(8)(e) CSA.

150 Art. 56(5)(a) CSA.

151 Art. 58(7)(a) and Art. 54(1)(j) CSA.

152 Art. 58(8)(a) CSA.

153 Art. 58(8)(b) and (d) CSA.

154 Art. 58(8)(c) CSA.

155 Art. 58(8)(e) CSA.

156 Art. 58(8)(e) CSA.

157 Art. 58 (7)(i) CSA.

158 Art. 58(7)(h) CSA.

159 Art. 58(9) CSA.

160 Art. 61 CSA.

161 Art. 61(4) CSA.

162 Art. 59 CSA.

163 Art. 58(7)(g) CSA.

164 Art. 58(4) CSA.

165 See Commission Implementing Decision M/536.

166 Art. 5(1)(a) RED.

167 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68.

168 Art. 6 Regulation 2018/1807.

169 See: Commission requests to ENISA on cloud and EU Common Criteria.

170 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

171 Art. 42 and 43 GDPR. Read further: Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman, Marc van Lieshout, & Gabriela Bodea, "Data protection certification mechanisms: Study on Articles 42 and 43 of the Regulation (EU) 2016/679", (1 ed.) Brussels: European Commission - DG Justice & Consumers (2019).

172 Art. 25 GDPR and 32 GDPR.

173 ENISA, *Handbook on Security of Personal Data Processing* (2017), https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing.

174 Other relevant legislation is the CE marking legislation: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415011406506&uri=CELEX:32008R0765, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415011214675&uri=CELEX:32008D0768

175 Public bodies (regulators) and their roles and competences are discussed in Chapter 2.

176 https://www.nen.nl/Standardization/Join-us/Technical-committees-and-new-subjects/TC-ICT/Financiele-diensten.htm

177 ISO/IEC 17065, clause 4.2.

178 Specific areas could be for example those that had a notification obligation for serious ICT-incidents under the 4th December 2017 Besluit (Besluit van 4 december 2017 tot aanwijzing van aanbieders van producten en diensten ten aanzien waarvan een plicht geldt om ernstige ICT-incidenten te melden – Besluit meldplicht cybersecurity), such as energy, drinkwater, nuclear, finance, electronic communications networks and ICT services, and critical infrastructures, or the operators of essential services according to the NIS Directive (Art. 4 and Annex II).

179 National Cybersecurity Agenda, a cyber secure Netherlands (2018) p.27f.

180 https://www.zeker-online.nl/partneringtrust/

181 https://www.securesoftwarealliance.org/about-secure-software-alliance/

182 https://www.zeker-online.nl/keurmerkhouders/: Twinfield; Reeleeze; Asperion; Informer; Business Software; Exact; Yuki; Flexkids; Tellow; Fleximaal; Loket.nl

183 https://www.zeker-online.nl/partneringtrust/

184 "Testing the security of components in the ENCS test lab," ENCS, https://encs.eu/activities/testing/encs-test-lab/.

185 KPMG, Export opportunities of the Dutch ICT sector to Germany (2017), 60f.

186 Examples of product and service providers are FoxIT providing a range of services including detection technologies, Magnet Forensics (https://www.magnetforensics.com/), or UCrowds, a start-up providing a crowd simulation software (https://www.ucrowds.com/).

187 See for example: https://www.aiginsurance.nl .

188 Source: Value Creation Company https://www.vcxc.com/en/themes/security_safety/#gallery

189 Centraal Bureau voor de Statistiek, Cybersecuritymonitor 2019, 7f, https://www.cbs.nl/nl-nl/publicatie/2019/37/cybersecuritymonitor-2019 .

190 ACM, *Incentive regulation of the gas and electricity networks in the Netherlands* (2017), 2.

191 Ibid, 3.

192 Ibid, 2.

193 For a complete overview of licensed Energy Suppliers in the Netherlands, see: https://www.acm.nl/nl/onderwerpen/energie/energiebedrijven/vergunningen/vergunninghouders-elektriciteit-en-gas.

194 Stichting Centraal Orgaan Voorraadvorming Aardolieproducten.

195 The legal basis for the role of NAM: Royal Decree of 30 May 1963, nr. 39 (Government Gazette 1963, 126). The legal basis for the role of COVA: Stockpiling Act (Wet voorraadvorming aardolieproducten 2012).

196 NIS Cooperation Group, Sectorial Implementation of the NIS Directive in the Energy Sector (2019).

197 Law of 2 July 1998, containing rules concerning the production, transport and supply of electricity (Electricity Act 1998).

198 Law of 22 June 2000, containing rules concerning the transport and supply of gas (Gas Act).

199 Law of 17 June 2013, containing rules regarding the supply of heat to consumers (Heat Act).

200 Law of 23 November 2006 amending the Electricity Act of 1998 and the Gas Act in connection with further rules regarding independent grid management.

201 For an overview of the applicable laws in the energy sector: <https://www.acm.nl/nl/onderwerpen/energie/wet--en-regelgeving/wet--en-regelgeving-energie>

202 ACM, Incentive regulation of the gas and electricity networks in the Netherlands, 3.

203 Regulation (EC) No 714/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity and repealing Regulation (EC) No 1228/2003 and Regulation (EC) No 715/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the natural gas transmission networks and repealing Regulation (EC) No 1775/2005.

204 Nederlandse Vereniging van Banken < https://www.nvb.nl >

205 Betaalvereniging Nederland https://www.betaalvereniging.nl >

206 Autoriteit Financiële Markten

207 De Nederlandsche Bank < https://www.dnb.nl >

208 Wet op het financieel toezicht (Wft)

209 Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)

210 Wet toezicht trustkantoren (Wtt)

211 Sanctiewet 1977 (Sw)

212 Directive (EU) 2015/2366 On Payment Services In The Internal Market, Amending Directives 2002/65/EC, 2009/110/EC And 2013/36/EU And Regulation (EU) No 1093/2010, And Repealing Directive 2007/64/EC (2015) (PSD2).

213 Article 4:24 Wft

214 AFM, 'Leidraad invulling van de Zorgplicht (semi)automatisch Vermogensbeheer' (2018) p. 15-16

215 See Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman, Marc van Lieshout, & Gabriela Bodea, "Data protection certification mechanisms: Study on Articles 42 and 43 of the Regulation (EU) 2016/679", (1 ed.) Brussels: European Commission - DG Justice & Consumers (2019).

216 The EU Regulation 1025/2012 recognised ISO, IEC, ITU, CEN, CENELEC, ETSI, and the national standardisation bodies.

217 See Chapter 3 of the Report for analysis of the EU Cybersecurity Act.

218 Also the requirements developed by ENCS for the energy sector can be positioned in this category.

219 For a systematic literature review, see: D. Ganji, C. Kalloniatis, H. Mouratidis, & S. M. Gheytassi, "Approaches to Develop and Implement ISO/IEC 27001 Standard-Information Security Management Systems: A Systematic Literature Review," *International Journal on Advances in Software* Volume 12, Number 3 & 4, (2019).

220 Read further: Paul de Hert, Vagelis Papakonstantinou & Irene Kamara, "The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection," *Computer Law & Security Review*, 32(1), (2016), 16-30; Eric Lachaud, "ISO/IEC 27701: Threats and opportunities for GDPR certification" (2020).

221 The scheme is available here: https://www.tuv-nederland.nl/common-criteria/documents/scheme-documentation.html

222 IEC 62433,TUV Nederland . Read further on the standard: Anastasios Arampatzis, "What Is the ISA/IEC 62443 Framework?" *Tripwire*, September 10, 2019, https://www.tripwire.com/state-of-security/regulatory-compliance/isa-iec-62443-framework/.

223 UNECE, *draft proposal for a Common Regulatory Framework on Cybersecurity* (2018), https://www.unece.org/fileadmin/DAM/trade/wp6/documents/2018/ECE_CTCS_WP.6_2018_9E_Cybersecurity.pdf

224 "ISO/IEC 19790:2012 Information technology — Security techniques — Security requirements for cryptographic modules," ISO, https://www.iso.org/standard/52906.html.

225 "Network Equipment Security Assurance Scheme (NESAS)," GSMA, https://www.gsma.com/security/network-equipment-security-assurance-scheme/.

226 "About 3GPP," 3GPP, https://www.3gpp.org/about-3gpp/about-3gpp.

227 "CIS Critical Security Controls," SANS, https://www.sans.org/critical-security-controls/.

228 NEN, *Commissieplan: Norm(sub)commissie 381027, Informatiebeveiliging, Cyber security en Privacy* (2017), https://www.nen.nl/Home_EN/Informatiebeveiliging-Cyber-security-en-Privacy.htm.

229 ETSI EN 303 645 V2.1.0, *Cyber Security for Consumer Internet of Things: Baseline Requirements*, REN/CYBER-0048 (2020).

230 ENISA, *Standards supporting certification, Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes* (2019).

231 Ibid.

232 See information about the DTS/CYBER-0050 specification at: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58434&curItemNr=39&totalNrItems=296&optDisplay=100000&qSORT=TB&qETSI_ALL=&SearchPage=TRUE&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qEND_CURRENT_STATUS_CODE=11+WI%3BM58&qSTOP_FLG=N&qKEYWORD_BOOLEAN=OR&qCLUSTER_BOOLEAN=OR&qCLUSTER=19&qFREQUENCIES_BOOLEAN=OR&qSTOPPING_OUTDATED=&butExpertSearch=Search&includeNonActiveTB=FALSE&includeSubProjectCode=FALSE&qREPORT_TYPE=

233 https://www.isaca.org/resources/cobit

234 See: https://www.pcisecuritystandards.org/document_library?category=educational_resources&document=pci_dss_large_org and https://managingrisktogether.orx.org/operational-risk-taxonomy/orx-reference-taxonomy-2019

235 The Netherlands National Communications Security Agency, Ministry of the Interior and Kingdom Relations represents the Netherlands in the SOG-IS.

236 Philippe Blot, Andreas Mitrakas, Aristotelis Tzafalias & Eric Vertillard, "Presentation at the ETSI Security Week" (Webinar, June 10, 2020), https://www.brighttalk.com/webcast/12761/409293?utm_source=brighttalk-presenter_screen&utm_medium=linkedin&utm_campaign=409293.

237 Ibid.

238 Aurelien Leteinturier et al, *CSPCERT WG (Milestone 3) Recommendations for the implementation of the CSP certification scheme* (2019).

239 Source: Eric Vetillard, "The Cloud services candidate scheme, presentation at ETSI Security Week", (June 11 2020);

240 Eric Vetillard, ETSI Security week 2020.

241 Ibid.

242 The classification is a way to present the findings. Some functions may be classified in more than one categories. Those functions are presented in the predominant category in this section.

243 See CCB: https://ccb.belgium.be/en/organisation

244 See National Cybersecurity Strategy Luxembourg (2018), objective 6: https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf

245 See: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

246 Luxembourg Institute for Standardisation, Accreditation, Security and the Quality of Products and Services (ILNAS).

247 https://english.ncsc.nl/get-to-work/become-a-partner

248 https://www.digitaltrustcenter.nl/over-het-digital-trust-center

249 https://www.ncsc.nl/onderwerpen/ransomware; https://www.ncsc.nl/actueel/beveiligingsadviezen

250 See Art. 43GDPR, Art. 21 Uitvoeringswet Algemene verordening gegevensbescherming, Informatieprotocol AP-RvA met betrekking tot accreditatie van AVG-certificeringsorganen Staatscourant 2020 (11507) and European Data Protection Board, Guidelines on Accreditation (p.9): https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-42018-accreditation-certification-bodies-under_en

251 A step-by-step description of the accreditation process and the roles of the RvA and the AP is provided here: https://www.rva.nl/nieuws/2018/avg-certificatie?highlight=AVG

252 This however is not currently the case, as it shows from the draft bill for the CSA.

253 https://www.rva.nl/onze-organisatie/over-de-rva

254 https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ahWG01/ahwg01_members

255 See NCSC "Cyber Security Consultancy Standard. Cyber Security Consultancy Standard" Version 1.3 (2019) https://www.ncsc.gov.uk/information/ncsc-certified-cyber-security-consultancy

256 https://www.ncsc.gov.uk/cyberessentials/overview

257 https://www.ncsc.gov.uk/section/products-services/ncsc-certification

258 The German Federal Office for Information Security (BSI) has developed a different type of certification called Beschleunigte Sicherheitszertifizierung" (BSZ, Accelerated Security Certification): https://www.bsi.bund.de/EN/Topics/Certification/product_certification/Accelerated_Security_Certification/Accelerated-Security-Certification_node.html

259 The vendors undertake to provide security updates if new vulnerabilities are uncovered.

260 https://www.dnb.nl/en/news/news-and-archive/nieuws-2017/dnb365801.jsp#

261 See legislative history of the proposal https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cybersecurity-competence-centers

262 See https://www.europa-nu.nl/id/vl9a5eao0ryr/nieuws/digital_priorities_for_future_of_eu?ctx=vhsjd8w6pdvc&s0e=vhdubxdwqrzw

263 The table is up to date until March 2020.