Tilt
Tilburg Institute
for Law, Technology,
and Society

Computer Security Incident Response Teams in the reformed Network and Information Security Directive: good practices

Irene Kamara and Jasper van den Boom

Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg Law School

The study is funded by the National Cyber Security Centre (NCSC-NL)

July 2022

Title	Computer Security Incident Response Teams in the reformed Network and Information Security Directive: good practices
Authors	Irene Kamara, Jasper van den Boom
Contributors	Kees Stuurman, Rosamunde van Brakel, Ronald Leenes
Research assistants	Thijs ten Caten, Abigaïl de Rijp
NCSC-NL project officer	Nouschka Auwema
Publisher	NCSC
Version	Final, 12 July 2022
TLP	White: Public

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the National Cyber Security Centre. The NCSC does not guarantee the accuracy of the data included in this study. Neither the NCSC nor any person acting on the NCSC's behalf may be held responsible for the use, which may be made of the information contained therein.

Table of Contents

Table of Tables

Table of Figures

Abbreviations

Agentschap Telecom	Radiotelecommunications Agency
AIVD	General Intelligence and Security Service
ANSSI	National Cybersecurity Agency of France
Bbni	Besluit beveiliging netwerk- en informatiesystemen
BITKOM	Digital Industry Association Germany
BMBF	Federal Ministry of Education and Research
BMI	Federal Ministry of the Interior and Community
BMWK	Federal Ministry for Economic Affairs and Climate Action
BMVg	Federal Ministry of Defence Germany
BSI	Federal Office for Information Security Germany
BSI Act	Act on the Federal Office for Information Security
CERT(s)	Computer Emergency Response Team(s)
CERT.at	Computer Emergency Response Team Austria
CERT-BUND	Computer Emergency Response Team Germany - BSI
CERT-EE	Estonian Information System Authority
CERT-EU	Computer Emergency Response Team for the EU Institutions, bodies and agencies
CERT-FR	Governmental centre for monitoring, alert and response to computer attacks
CSIRT(s)	Computer Security Incident Response Team(s)
CVD	Coordinated Vulnerability Disclosure
CFCS	Centre For Cyber Security - Denmark
DCIS	Decentralized Information Security Units
EGC	European Government CERTs Group
ENISA	European Union Agency for Network and Information Security
EU	European Union
FIRST	Forum of Incident Response and Security Teams
GFCE	Global Forum on Cybersecurity Expertise
GmbH	Company with limited liability
GovCERT	Government Computer Emergency Response Team
IBD	Information Security Service
ICT	Information and Communications Technologies
InterCERT France	non-profit organisation which constitutes the first CSIRT community in France
ISAC(s)	Information Sharing and Analysis Centre(s)
IWWN	International Watch and Warning Network
LDS	System of National Coverage
MISP	Malware Information Sharing Platform
MIVD	Military Intelligence and Security Service
NATO	North Atlantic Treaty Organization
NCSC(-NL)	National Cyber Security Centre (of the Netherlands)
NCTV	National Coordinator for Counterterrorism and Security

NIS Directive / NISD1	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
NIS2 Directive / NISD2	Compromise agreement text of 17 June 2022 directive on measures for a high common level of cybersecurity across the Union
NIS Gesetz	Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen
NIS-Office(s)	Office(s) for Strategic Network and Information Security
NLO Network	National Liaison Officers Network
NSS	Net Security Service
OES	Operators of Essential Services
RIA	Information Systems Authority – Estonia
RPA	Robotic Process Automation
SME(s)	Small- and Medium Enterprise(s)
SOCTA	Serious and Organised Crime Threat Assessment
TF-CSIRT	Task Force on Computer Security Incident Response Teams
UP KRITIS	Public-private cooperation between operators of critical infrastructures, their associations and the responsible government agencies
Wbni	Wet Beveiliging Netwerk- en Informatiesystemen

Executive summary

The Cybersecurity landscape is ever changing and evolving. The speed with which the field is moving was obvious from the reform of the 2016 Network and Information Security Directive, which took place only a few years after the NIS1 was transposed to national legislation of the Member States. Changes in cybersecurity law are geared by the development of technologies, the growing reliance and dependence on information and security networks, and the new ways attackers exploit vulnerabilities and launch their cyber-attacks, and the effectiveness of the existing legislation. After a two-year legislative process, political agreement on NIS2 took place in May 2022.

Following the recent reform of the EU Network and Information Security Directive, the study aimed at identifying the changes in the requirements and tasks of the Computer Security Incident Response Teams and good practices in the performance of their tasks and organisation. The study looked into six CSIRTs: NCSC in the Netherlands, CERT.at in Austria, CERT-FR in France, CERT-Bund in Germany, CERT-EE in Estonia, and the Center For Cyber Security in Denmark. The desktop analysis showed that CSIRTs are usually organised as distributed, centralised, or coordinating teams, with several variations. With regard to the service offered by CSIRTs those are of reactive nature (such as incident response), proactive nature (such as proactive scanning of networks) and quality management services e.g. as training.

The legal analysis of the new NIS2 in comparison to the NIS1, showed that tasks and competences of CSIRTs have been considerably upgraded in NIS2. This is not only due to the broadening of the scope to the Directive, but also the type of CSIRT tasks. For example, the range of tasks and powers of CSIRTs has been expanded from monitoring and analysing incidents to providing assistance to entities, collecting and analysing forensic data and providing risk and incident analyses. In addition, the tasks Coordinated Vulnerability Disclosure (CVD) and proactive scanning of public networks have been added to the tasks of CSIRTs in NIS2.

Following these analyses and the comparison, the study explored the operational and legal framework for the NCSC in the Netherlands. The NCSC-NL performs the national CSIRT tasks and falls under the responsibility of the Ministry of Justice and Security. The NCSC carries out incident response tasks, facilitates and promotes national and international cooperation and acts as an information sharing partner.

An important part of this research revolved around investigating good practices of CSIRTs in other Member States. These good practices were divided into incident response, international and national cooperation, and technical research and monitoring.

The key findings of the study:

- The approaches to fulfilling CSIRT tasks under NIS2 diverge strongly from one another, as do the identified good practices across Member States. However, the identified good practices are most often not mutually exclusive.
- Most of the interviewed Member States face a large growth of constituencies with the introduction of NIS2 and are currently in the process of developing strategies to accommodate new sectors and entities in their methods to perform CSIRT tasks.

- The most common problems that are faced in amending strategies revolve around scalability, ensuring access to CSIRT services for new entities in the scope of NIS2, and preventing coordination risks.
- The largest differences between Member States are their centralized or decentralized approaches in the organization of (national) CSIRTs, the use of risk-based or sector-based approaches to identify and respond to threats and different forms of automation that may include portals for information sharing, notifications or tools for pro-active scanning.
- Scalability is a prominent issue as not all CSIRTs have (yet) access to the necessary resources and personnel to deal with the increase in constituencies. Expanding the CSIRT and hiring new personnel may not be possible due to a lack of resources or a lack of candidates with the right skills and qualifications. Possible solutions for issues related to scalability may be found with automation and the standardization of protocols to use resources more efficiently, and/or by offering training programs to attract new talent.
- The use of automated tools for scanning or information sharing must happen in accordance with fundamental rights of citizens, including the right to privacy and data protection. Reliance on automated tools - in particular those for scanning - should be limited in their use and subjected to strict tests of proportionality and necessity.
- Ensuring access to CSIRT services for the constituency may arise in both centralized and decentralized approaches. Member States that rely on centralized approaches may not have the available resources, while Member States with a decentralized approach may not have set up a sectoral CSIRT for the new NIS2 entities or may not be able to find private parties that have the capabilities.
- Reliance on an ecosystem of accredited and certified private actors may help CSIRTs to scale up and provide a cost-efficient way to ensure access to CSIRT services for constituents in new sectors under NIS2.
- Different approaches require the national CSIRT to fulfil different roles. The Member State must ensure that it is clear for the entities and potential public or private CSIRTs which roles the national CSIRT fulfils.

Samenvatting

Het cyberbeveiligingslandschap is voortdurend in beweging en onderhevig aan verandering. De snelheid waarmee dit rechtsgebied evolueert blijkt uit de huidige hervorming van de netwerk- en informatiebeveiligingsrichtlijn die werd geïntroduceerd in 2016. De herziening vindt slechts enkele jaren plaats na de implementatie van NIB1 in nationale wetgeving.
Veranderingen in de cyberbeveiligingswetgeving worden gestuurd door ontwikkelingen in de stand van de technologie, de toenemende afhankelijkheid van informatie- en beveiligingsnetwerken, de nieuwe manieren waarop cyberaanvallers online kwetsbaarheden uitbuiten en aanvallen lanceren en de doeltreffendheid van de bestaande wetgeving. Na een wetgevingsproces van twee jaar werd in mei 2022 een politiek akkoord bereikt over NIB2.

Naar aanleiding van de recente hervorming van de Netwerk- en informatiebeveiligingsrichtlijn van de EU werd met deze studie beoogd de veranderingen in de eisen en taken van de Computer Security Incident Response Teams en ‘good practices’ bij de uitvoering van hun taken en organisatie in kaart te brengen. In de studie werden zes CSIRT's onder de loep genomen: NCSC in Nederland, CERT.at in Oostenrijk, CERT-FR in Frankrijk, CERT-Bund in Duitsland, CERT-EE in Estland en het Center For Cyber Security in Denemarken. Uit deskresearch bleek dat CSIRT's gewoonlijk zijn georganiseerd als gedistribueerde, gecentraliseerde of coördinerende teams met verschillende variaties. De door de CSIRT's aangeboden diensten zijn van reactieve aard (zoals respons op incidenten), proactieve aard (zoals proactief scannen van netwerken) en diensten op het gebied van kwaliteitsbeheer, bijv. in de vorm van training.

Uit de juridische vergelijkende analyse tussen de nieuwe NIB2-richtlijn en de NIB1-richtlijn is gebleken dat de taken en bevoegdheden van de CSIRT's in NIB2 aanzienlijk zijn uitgebreid. De reden hiertoe is niet alleen de verruiming van het toepassingsgebied van de richtlijn, maar ook aan het soort CSIRT-taken. Zo is het takenpakket en de bevoegdheid van de CSIRT's uitgebreid van het monitoren en analyseren van incidenten naar het verlenen van bijstand aan entiteiten, het verzamelen en analyseren van forensische gegevens en het verstrekken van risico- en incidentanalyses. Bovendien zijn de taken "Coordinated Vulnerability Disclosure" (CVD) en het proactief scannen van openbare netwerken toegevoegd aan de taken van de CSIRT's in NIB2.

Naar aanleiding van deze analyses en de vergelijking is in de studie het operationele en juridische kader voor het NCSC in Nederland verkend. Het NCSC-NL voert de nationale CSIRT-taken uit en valt onder de verantwoordelijkheid van het Ministerie van Justitie en Veiligheid. Het NCSC voert incidentresponstaken uit, faciliteert en bevordert nationale en internationale samenwerking en treedt op als informatie-uitwisselingspartner.

Een belangrijk deel van dit onderzoek betreft het onderzoeken van 'good practices’ van CSIRT's in andere lidstaten. Deze 'good practices’ zijn onderverdeeld in reactie op incidenten, internationale en nationale samenwerking, en technisch onderzoek en toezicht.

De belangrijkste bevindingen van de studie zijn:

- De methoden voor de uitvoering CSIRT-taken in het kader van NIB2, evenals de vastgestelde 'good practices', verschillen sterk van elkaar per lidstaat. De vastgestelde 'good practices' sluiten elkaar echter meestal niet uit.
- De meeste geïnterviewde lidstaten krijgen met de invoering van NIB2 te maken met een sterke groei van het aantal entiteiten en werken momenteel aan

strategieën om nieuwe sectoren en entiteiten op te nemen in hun methoden om CSIRT-taken uit te voeren.

- De meest voorkomende problemen bij het wijzigen van strategieën hebben betrekking op opschaalbaarheid, het garanderen van toegang tot CSIRT-diensten voor nieuwe entiteiten in het toepassingsgebied van NIB2 en het voorkomen van risico's in de coördinerende taken.
- De grootste verschillen tussen de lidstaten zijn hun gecentraliseerde of gedecentraliseerde aanpak bij de organisatie van (nationale) CSIRT's, het gebruik van risicogebaseerde of sectorgebaseerde benaderingen om bedreigingen vast te stellen en erop te reageren, verschillende vormen van automatisering van portalen voor informatie-uitwisseling, kennisgevingen of instrumenten voor proactief scannen.
- Opschaalbaarheid is een belangrijk punt, aangezien (nog) niet alle CSIRT's over de nodige middelen en het nodige personeel beschikken om de toename van het aantal entiteiten op te vangen. Uitbreiding van CSIRT's en werving van nieuw personeel is wellicht niet mogelijk door een gebrek aan middelen of een gebrek aan kandidaten met de juiste vaardigheden en kwalificaties. Mogelijke oplossingen voor problemen in verband met opschaalbaarheid kunnen worden gevonden in automatisering en standaardisering van protocollen om de middelen efficiënter te gebruiken, en/of door opleidingsprogramma's aan te bieden om nieuw talent aan te trekken.
- Het gebruik van geautomatiseerde instrumenten voor het scannen of delen van informatie moet gebeuren met inachtneming van de grondrechten van de burgers, waaronder het recht op privacy en gegevensbescherming. Het gebruik van geautomatiseerde instrumenten - met name die voor scanning - moet worden beperkt en aan strikte evenredigheids- en noodzakelijkheidstoetsen worden onderworpen.
- Het waarborgen van de toegang tot CSIRT-diensten voor de achterban kan zich zowel bij een gecentraliseerde als bij een gedecentraliseerde aanpak voordoen. Lidstaten die gebruik maken van een gecentraliseerde aanpak beschikken wellicht niet over de beschikbare middelen, terwijl lidstaten met een gedecentraliseerde aanpak wellicht geen sectoraal CSIRT voor de nieuwe NIB2-entiteiten hebben opgezet of geen particuliere partijen kunnen vinden die over de benodigde capaciteiten beschikken.
- Het opbouwen van een ecosysteem van vertrouwen van geaccrediteerde en gecertificeerde particuliere actoren kan de CSIRT's helpen op te schalen en kan een kostenefficiënte manier zijn om de toegang tot CSIRT-diensten voor onderdelen in nieuwe sectoren in het kader van NIB2 te waarborgen.
- Verschillende benaderingen vereisen dat het nationale CSIRT verschillende rollen vervult. De lidstaat moet ervoor zorgen dat het voor de instanties en potentiële publieke of particuliere CSIRT's duidelijk is welke rol het nationale CSIRT vervult.

1. Introduction

1.1 Background and aims of the study

Most organisations today rely on networks and information systems. Those are however vulnerable to security threats that arise from technical failures, but also from organised crime activities targeting citizens, businesses, and critical infrastructure. Ransomware, DDoS, and malware are often offered as a service and can be purchased online by cybercriminals. The digital transformation of society, heightened by COVID-19, intensified and expanded the threat landscape.

As Europol outlines in its 2021 SOCTA Report, critical infrastructure is expected to continue to be targeted by cybercriminals in the forthcoming years, which poses financial and social risks.[1] Data leakage, phishing, and extortion of organisations' data are ranked among the highest threats in the Netherlands.[2] Computer Incident Response Teams have a pivotal role in both proactively and reactively contributing to the overall cybersecurity level of entities.

In the European Union, the Network and Information Security Directive 1148/2016 (NIS Directive) was adopted as part of the EU Cybersecurity Strategy. The NIS Directive laid down measures with the intention to achieve a high common level of security of network and information systems within the Union to improve the functioning of the internal market. The NIS Directive aimed at improving the cybersecurity capabilities of Member States at domestic level, increasing the level of EU cooperation, and establishing supervision mechanisms of the cybersecurity of operators of essential services and digital service providers.

While the impact of the NIS1 Directive has been significant, the Commission impact assessment showed that improvements are necessary. More specifically, the scope of the NIS Directive was found to be limited in terms of the sectors covered, diversity in the reporting duties of Member States had negative consequences on the cyber-resilience at national and European level, and cooperation and active information sharing among authorities of Member States was insufficient. Moreover, the supervision and enforcement regime of the NIS Directive was found to be ineffective.[3]

In 2020, following the results of the assessment, the European Commission published a Proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS2). The NIS2 has three pillars: Member State capabilities, risk management, and cooperation and information exchange. The draft NIS2 Directive proposed several changes in relation to the current NIS Directive, which are expected to have significant impact on the scope and effectiveness of the existing cybersecurity measures.[4] As a result, changes with respect to tasks and responsibilities of actors and entities in the cybersecurity domain are necessary at domestic level

[1] Europol, 'European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021. A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime' (December 2021).<https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf> Accessed 20 June 2022.

[2] Deloitte, 'Cyber security in the Netherlands: a responsibility we share. Dutch cyber security survey' (2021). <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-dutch-cyber-security-survey-executive-summary.pdf> Accessed 20 June 2022.

[3] Explanatory Memorandum to NISD1 2016, p. 6.

[4] See political agreement text of NIS2: https://data.consilium.europa.eu/doc/document/ST-10193-2022-INIT/x/pdf Accessed 20 June 2022.

in every Member State, with the aim to respond to higher needs and expectations created with the proposed Directive.

The Netherlands follows a decentralised model in the distribution of competences in the field of cybersecurity. NCSC-NL (NCSC) is a key player in this landscape, providing skills and expertise both to its regulated entities and to other CSIRTs beyond the country's borders. It acts as Single Point of Contact, CSIRT, supports Operators of Essential Services, performs technical analysis and research, information dissemination and other tasks. Other actors include the Radiotelecommunications Agency (Agentschap Telecom), the General Intelligence and Security Service (AIVD), the National Bureau for Security Connections, the Military Intelligence and Security Service (MIVD), and the Digital Trust Centre (Kamara et al, 2020).[5]

1.2 Research question, approach, and methodology

Against this backdrop, the NCSC has requested a study with the main research question being "What impact is the new NIS Directive expected to have on the CSIRT tasks and responsibilities of the NCSC?" This study, therefore, aims at identifying the upcoming changes and offer insights into the modus operandi of national cybersecurity authorities and CSIRTs of other Member States. The study essentially concerns an analysis of the expected effects on tasks, responsibilities, and approach of NCSC CSIRT tasks as a result of the expanded scope to be introduced by NIS2, such as an expected increase in the number and types of entities (constituencies) falling within the ambit of the NIS2, and possibly the NCSC.[6] The report outlines the changes in tasks and responsibilities following the NIS2 and reflects on good practices and future organisational and implementation plans in different EU Member States.

The research team conducted literature review and legal doctrinal analysis to analyse the changes in the change of the legal framework, with the reform of the NIS Directive. Policy and guidance documents at national and EU level, were analysed for the desktop research, next to literature. The research also involved empirical methods. First, there was a non-structured interview with two NCSC employees, to calibrate the focus of the study and test the preliminary desktop research findings. Next, a focus group with NCSC employees from different units and backgrounds (operational, organisational, policy) took place in March 2022 online. The focus group discussed perceived opportunities and challenges with the impact of the NIS2 Directive on how the NCSC performs its CSIRT tasks. The expert focus group discussions were directed towards three themes and four aspects. The themes emerged from the legal analysis of the CSIRT tasks in the NIS Directive and the 2020 Commission Proposal for the NIS reform:

1. Incident response
2. Information and knowledge sharing
3. Technical monitoring and research

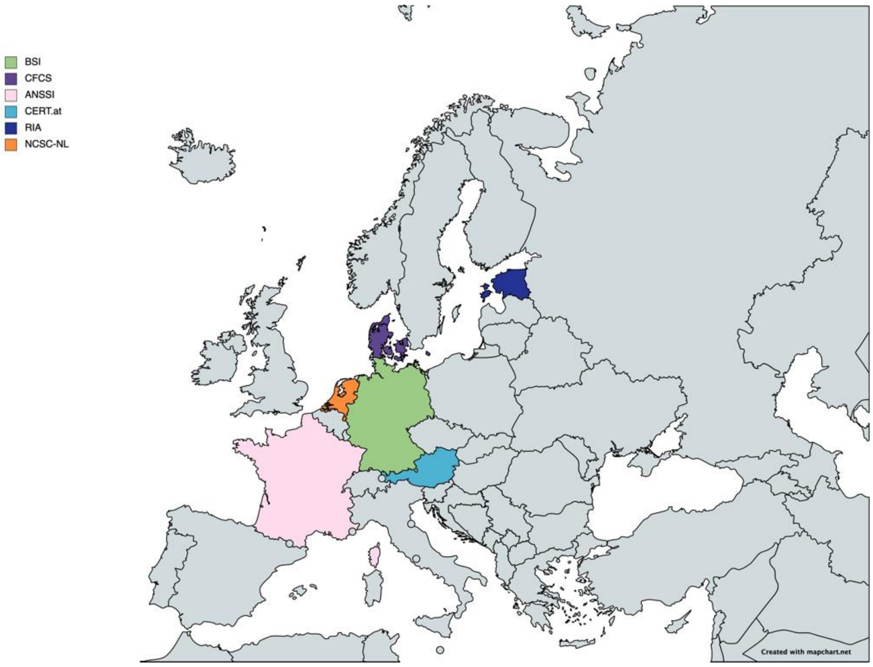
[5] I. Kamara and others, 'The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act' (July 2020). < file:///C:/Users/Gebruiker/Downloads/NCSC_CYBERCERT_FinalReport__20200730.pdf> Accessed 20 June 2022.
[6] See Section 3 for the analysis of the Network and Information Security Directive 2.

To further specify and stir the discussion in the focus group, each theme addressed four aspects, as identified in the CSIRT maturity assessment literature[7]:

Organisation	Concerns the foundation and scope of CSIRT activities
Human	Concerns the CSIRT staff, technical and non-technical, and their role in assisting the CSIRT achieving its tasks
Processes	Concerns the processes that are in place for the CSIRT to perform its tasks.
Tools	Concerns the tools and technologies used by the CSIRT to serve its constituency.

While the focus group and in general the research for this study does not aim to conduct a full-scale assessment of the preparedness of the NCSC-NL, the outcomes of the research will inform such an exercise, since they are following the rationale of the ENISA maturity assessment framework.

Following the focus group outcomes, an interview protocol was drafted for conducting interviews with representatives of cybersecurity centres and CSIRT teams in different Member States. The interviews with the selected MS were semi-structured and followed the themes and aspects validated in the focus group. There were in total six interviews conducted online with ten representatives from five Member States in March and April 2022.[8] The selection of the Member States was proposed by the NCSC-NL and agreed by the research team. In specific, Austria, Denmark, and Estonia were selected inter alia due to their different models of operation and existing large number of constituencies already under NIS Directive, while Germany and France, were selected due to their well-established and mature CSIRT teams.



[7] ENISA, 'CSIRT Maturity Assessment Framework – Updated and improved' (February 2022). < https://resilientshield.nl/wp-content/uploads/2022/03/ENISA-CSIRT-Maturity-Framework-Updated-and-improved_ResilientShield.pdf> Accessed 20 June 2022.

[8] See Annex 3.

Figure 1: Map distribution of interviewed organisations

Due to timeline and the scope of the research, the study is not exhaustive, but focuses on deciphering good practices. A 'good practice' for the purposes of this study is an activity, process, approach, model, tool, or other mechanism in a broad sense, which falls under one or more of the identified themes of incident response, information sharing, and technical monitoring, that a national CSIRT of an EU Member State considers itself as successful in achieving its tasks under the Network and Information Security Directive and recommends it to other CSIRTs within its network.[9] A first list of identified good practices were reviewed internally from the research team and presented at the NCSC in a second focus group in June 2022. The EU and national cybersecurity landscape, the NIS framework, the changes in the CSIRT tasks under NIS2, and the analysis of how selected relevant other Member State's NCSCs operate and plan to prepare in view of the legal reform, provided the background for the identification of good practices.

The scope of this study does not cover per se concrete organisational recommendations and strategic advice on operational aspects of the NCSC, capacity, personnel, and training issues as such. Those issues are touched upon in the framework of the desktop and empirical research. The study does not cover the impact of NIS2 on regulated entities, such as large industry or start-ups.

The study is up-to-date until 17 June 2022.

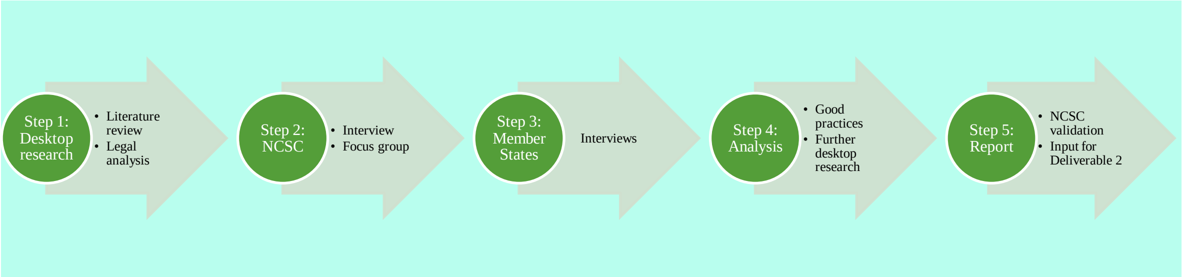


Figure 2: Overview of methodology steps

1.3 Structure of the report

Following the Introduction, Section 2 provides a brief overview of the most common typologies of organisation of CSIRT teams and the breadth of offered services and competences. While each CSIRT, especially the national ones, are organised in different way, accommodating national specificities and legal requirements, the general models do not differ greatly. Sections 3 and 4 analyse the key changes in the tasks and responsibilities of CSIRTs under NIS2. The following Section 5 presents the Dutch emergency response landscape and the Dutch legislation, transposing the NIS1 in the Dutch legal order. Section 6 provides the comparative analysis of the operational environment and organisational models of the CSIRTs in the selected countries: Austria, Denmark, Estonia, France, and Germany. Section 7 presents the analysis of the identified good practices in 1) Incidents response 2) International cooperation and information sharing, and 3) Technical monitoring and research. Section 8 provides a discussion of the findings and concludes the Report.

[9] Olivier Serrat, *Knowledge Solutions* (Springer 2017), 843-846.

2. Typologies of organisational models and services of CSIRTs

CSIRTs have evolved to be the backbone of cybersecurity of networks and information systems, often compared by analogy to a fire brigade, intervening in emergencies to support and provide assistance, but also ensure there are proper lessons learned and shared after incidents have occurred. CSIRTs, originally called Computer Emergency Response Teams (CERTs), [10] are teams with "appropriately skilled and trusted members of the organization that handles incidents during their lifecycle".[11] A national CSIRT, as opposed to other regular CSIRTs, has a national scope, is recognised by the national government, and is usually the main contact point for external relations and other CSIRTs teams of other countries. The following section provides an overview of organisational model typologies and CSIRT service inventories, most often encountered in literature.

Organisational models of CSIRTs

	FIRST	Carnegie Mellon	NIST	OAS	Others
Distributed	Embedded model	Internal distributed model	Distributed incident response CSIRT model	Distributed CSIRT model	
Centralised	-	Internal centralised CSIRT model	Central Incident Response CSIRT model	Centralised CSIRT model	Regional/Vendor/ Sectoral CSIRT model
Coordinating	Campus model	Coordinating CSIRT model	Coordinating CSIRT model	Coordinating CSIRT model	National CSIRT model
Organisational	Independent business model	-	-	Localised security team model	Organisational/ Commercial CSIRT model
Others	-	Internal Combined Distributed and Centralised CSIRT	-	-	-

Table 1: overview of organisational models of CSIRTs

2.1. FIRST CSIRT Models and services

FIRST is the Forum of Incident Response and Security Teams, established in 1989, an international non-governmental forum, comprised of CSIRTs from all over the world. Its aim is to bring together CSIRTs from public administration, commercial, and academic sectors, and facilitate the collaboration and exchange of information, best practices, and tools for incident handling.[12] Members are admitted to FIRST by the nomination of two existing members and the approval of 2/3 of all FIRST Members.

[10] Isabel Skierka and others, 'CSIRT basics for policymakers. The History, Types & Culture of Computer Security Incident Response Teams' (2015). Working paper May 2015 <https://www.gppi.net/media/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf> Accessed 20 June 2022.

[11] ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management (the standard is currently under revision).

[12] FIRST, 'Bylaws of FIRST.Org, Inc.' (2022). <https://www.first.org/about/policies/bylaws> Accessed 20 June 2022.

The FIRST 'Establishing a CSIRT' guidance provides for three organisational models for CSIRTs:[13]

- **Independent business model**: The CSIRT is an independent organisation with own management, employees, and network.
- **Embedded model**: In this model, the CSIRT is part of another organisation. This may further include a centralised or a de-centralised model, where CSIRT teams are in one or more locations.
- **Campus model**: In this model, participating members either do not have their own CSIRT team or they may have an own CSIRT team. In any case, there is also a 'mother' or 'core' CSIRT, which coordinates the efforts and acts as the point of contact. The core CSIRT may itself be an independent or embedded organisation, following one of the previous models.

As regards the services, incident handling includes the following steps:

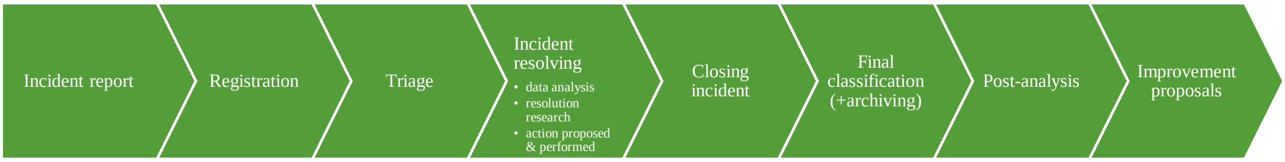


Figure 3:Incident Handling Process Workflow (FIRST.org)

Next to Incident Handling, the CSIRT may provide other reactive services such as alerts and warnings, vulnerability handling, artifact handling, proactive services such as technology watch, development of tools, intrusion detection and scanning services, and lastly security quality management services such as awareness raising, product certification, and training.[14]

2.2 Carnegie Mellon Organisational models for CSIRTs

Another commonly used source for CSIRTs organisational models is the Carnegie Mellon resources, especially the CSIRTs Handbook,[15] which provides the following organisational models for a CSIRT:

- **Internal Distributed CSIRT:** In this model, the organisation uses existing staff to provide a distributed CSIRT to deal with incident response.
- **Internal Centralised CSIRT:** In this model, a fully staffed and dedicated CSIRT is providing incident response.
- **Internal Combined Distributed and Centralised CSIRT:** The model is a combination of the previous two models, having a centrally located dedicated team and existing staff or teams in strategic locations through an organisation or other organisations.
- **Coordinating CSIRT:** In this model, the CSIRT has no authority over the members of its constituency, it coordinates and facilitates the handling of incidents in different organisations.

[13] Martijn van der Heide, 'Establishing a CSIRT' (November 2017), version 1.2. < https://www.first.org/resources/guides/Establishing-CSIRT-v1.2.pdf> Accessed 20 June 2022.
[14] FIRST, 'Computer Security Incident Response Team (CSIRT) Services Framework' (2019). <https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1> Accessed 20 June 2022.
[15] Georgia Killcrece and others, 'Organizational Models for Computer Security Incident Response Teams (CSIRTs)' (December 2003). < https://resources.sei.cmu.edu/asset_files/handbook/2003_002_001_14099.pdf> Accessed 20 June 2022.

As regards the services, the Handbook, like FIRST, categorises the CSIRTs services into i) **reactive**, namely incident handling, vulnerability handling, and artifact handling, ii) **proactive** services, such as technology watch, development of security tools, security related information dissemination, security audits or assessments, and iii) **security quality management services**, such as risk analysis, business continuity and disaster recovery planning, awareness building, product certification, and others. ENISA, in its 2020 Guidance on how to establish a CSIRT and a Security Operations Centre (SOC),[16] uses the FIRST service framework.

2.3 NIST CSIRT Models and services

The US National Standardisation Institute (NIST) in its Computer Security Incident Handling Guide [17] has identified, along the same lines with the previous sources, the following organisational structure models for CSIRTs:

- **Central Incident Response CSIRT:** In this model, one central CSIRT handles all the incidents.
- **Distributed Incident Response CSIRT:** In this model there are several CSIRTs responsible for different segments of an organisation or types of incidents and constituencies.
- **Coordinating CSIRT:** In this model, the CSIRT provides advice to other teams, but does not have a supervisory or oversight role.

NIST recognises that the primary role of a CSIRT is Incident Response but also acknowledges the multifaceted role of a CSIRT in ensuring cybersecurity. In that sense, next to incident response, a CSIRT may offer advisory services for vulnerabilities and threats, information sharing with ISACs or regional information sharing groups, and education and awareness.

2.4 OAS Best practices for National CSIRT establishment

The best practices guide developed by the Organisation of American States,[18] identifies four main organisational structures for CSIRT:

- **Localised security team:** This model does not involve an established CSIRT but implies that the security incidents are handled by the security team of an organisation.
- **Distributed CSIRT:** Similarly, to the Carnegie Mellon model, on which the OAS best practices models are based, this model implies that the CSIRT has a coordinating team and several comprehensive response centres geographically distributed. The duties are per CSIRT are divided according to knowledge, location where incidents occur, and the affected target. The coordinating team establishes standardised processes and good practices, seeks to increase synergies, and maintains statistics.

[16] ENISA, ʼHow to setup up CSIRT and SOC. Good Practice Guideʼ (December 2020

[17] Paul Cichonsk and others, ʼComputer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technologyʻ (August 2012), Special Publication 800-61, Revision 2. <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf￼> Accessed 20 June 2022.

[18] Organization of American States, ʼBest Practices for Establishing a National CSIRTʻ (April 2016). <￼￼ https://www.thegfce.com/good-practices/documents/publications/2016/04/01/best-practices-for-establishing-a-national-csirt> Accessed 20 June 2022.

- **Coordinating CSIRT:** This is a similar model to the previous one, with the difference that the coordination focuses on the effective response to incidents i.e. synergy between response centres.
- **Centralised CSIRT:** This model foresees a single CSIRT for the management and response to incidents across different locations. Usually, in such models the CSIRT also interacts with specialists on products or services.

Further, it is interesting to note that the guide classifies CSIRTs by the sector or the community they serve. Next to national CSIRTs, the guide identifies critical infrastructure CSIRTs, academic, commercial, government, small medium enterprise (SME) CSIRTs, and others.

Other sources,[19] also recognise the distinction between the following CSIRT types:

- **National CSIRT**, which are the main contact point for the country and the end responsible for domestic incident response.
- **Sectoral CSIRT,** which serve specific sectors. Those may act only as information sharing platforms i.e. ISACs or also conduct incident response.
- **Organisational CSIRT,** are responsible for monitoring and responding to incidents in the organisational to which they belong, e.g. in a private company.
- **Commercial CSIRT,** are CSIRTs that offer professional incident response services to other organisations.
- **Regional CSIRT,** are CSIRTs that handle incident response in a specific region, either within a country or cross-border.
- **Vendor CSIRT,** which are CSIRTs for vendors of IT systems or products used by individuals or commercial entities.

2.5 ENISA CSIRT setting up Guide

ENISA's 2006 Guide[20] provides CSIRT organisational models similar to FIRST: namely 1) the independent business model 2) the embedded model, and 3) the campus model. The guide also adds the voluntary model, whereby a group of specialists provide advice and support to each other on a voluntary basis.

Services of CSIRTs

	FIRST CSIRT	Carnegie Mellon	NIST
Reactive services	1. Incident report acceptance	1. Alerts & warnings 2. Incident analysis	1. Incident handling 2. Vulnerability handling

[19] Global Forum on Cyber Expertise, 'GFCE Global Good Practices. National Computer Security Incident Response Teams (CSIRTs)' (2017), Global Conference on Cyber Expertise 2017. <https://thegfce.org/wp-content/uploads/2020/06/NationalComputerSecurityIncidentResponseTeamsCSIRTs-1.pdf> Accessed 20 June 2022; Global Forum on Cyber Expertise, 'Launch of the Global Forum on Cyber Expertise. 16 April 2015. The Hague Declaration on the GFCE' (April 2015). <https://thegfce.org/wp-content/uploads/2020/04/the-hague-declaration-on-the-gfce.pdf> Accessed 20 June 2022 & Isabel Skierka and others, 'CSIRT basics for policymakers. The History, Types & Culture of Computer Security Incident Response Teams' (2015). Working paper May 2015 <https://www.gppi.net/media/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf > Accessed 20 June 2022.

[20] ENISA, 'A step-by-step approach on how to setup a CSIRT. Including examples and a checklist in form of a project plan' (2006), Deliverable WP2006/5.1(CERT-D1/D2). <https://www.enisa.europa.eu/publications/csirt-setting-up-guide> Accessed 20 June 2022.

	2. Alerts & warnings 3. Vulnerability discovery 4. Vulnerability response 5. Artifact handling 6. Incident analysis 7. Artifact & forensic evidence analysis 8. Mitigation & recovery 9. Incident coordination 10. Crisis management support	3. Incident response 4. Incident support 5. Incident response coordination 6. Vulnerability analysis 7. Vulnerability response 8. Artifact analysis 9. Artifact response	3. Threat handling 4. Information sharing
Proactive services	1. Technology watch 2. Development of tools 3. Intrusion detection & scanning services 4. Monitoring	1. Announcements 2. Technology watch 3. Security audit or assessments 4. Configuration & maintenance of security tools, applications and infrastructures 5. Development of security tools 6. Security related information dissemination 7. Security audits or assessments 8. Intrusion detection	1. Intrusion detection
Security quality management services	1. Awareness raising 2. Data acquisition 3. Analysis and synthesis 4. Communication 5. Product certification 6. Training & education 7. Exercises 8. Technical & policy advisory	1. Risk analysis 2. Business continuity & disaster recovery planning 3. Security consulting 4. Awareness raising 5. Ecucation & training 6. Product certification	2. Education 3. Awareness raising

Table 2: Overview of services of CSIRTs

3. The Network and Information Security Directive and its 2022 reform

Having identified organisational models and types of services usually offered by CSIRTs worldwide in the previous Chapter, this Chapter analyses the legal framework and requirements in the European Union law on Network and Information Security. The Network and Information Security Directive was adopted in 2016 with a two-year transposition period. The NIS1[21] aimed at achieving and maintaining a high level of security of network and information security systems and improve the functioning of the Internal Market. To that end, the NIS1 included five important pillars:

1. The identification of operators of essential services
2. Obligations for Operators of Essential Services and Digital Service Providers
3. Cooperation provisions
4. Standardisation aspects and
5. National frameworks and strategies on the security of network and information security systems.

The evaluation of the NIS1 however showed several issues that required its revision. Those included the divergent security and reporting requirements of entities in different Member States, the ineffective supervision and enforcement, limited information sharing between Member States, but also uneven resources for competent authorities. On the last point, the Commission reported that the financial and human resources especially for CSIRTs, and the resulting different levels of maturity, varied significantly.[22]

One of the important distinctions in the NIS1 is the concept of operators of essential services and the digital service providers. Operators of essential services (OES) are public or private entities in the sectors and types referred to in the Annex II of the Directive, as shown in Table 3, that fulfil three cumulative criteria:[23]

1. *The entity would provide a service that is essential for the maintenance of critical societal and/or economic activities*
2. *the provision of that service depends on network and information systems, and*
3. *an incident would have significant disruptive effects on the provision of that service.*

Under NIS2, the concept of operators of essential services has changed to "essential services" and the list of sectors, subsectors, and types of providers was broadened significantly. This broadening of the scope of the entities that fall under the scope of the NIS2 has a direct impact on the number of constituency should be benefitted and assisted by CSIRTs, such as the NCSC-NL.[24] An important difference with NIS1 is the abolishment of the identification of the OES by the Member States in their own territories. Under NIS2, the identification process is replaced by a list of

[21] 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.

[22] European Commission, 'Commission staff working document – Impact Assessment Report – Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', SWD (2020) 345 final.

[23] NIS1, art. 5.

[24] Inspectie Justitie en Veiligheid, Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021 (June 2021), 8

requirements and the entities designated in the Annex of the NIS2. In this way, the discrepancies in the types of entities identified in NIS1 across Member States are aimed to be eliminated.[25]

NIS1		NIS2	
Sector	**Subsector**	**Sector**	**Subsector**
Energy	Electricity, oil, gas	Energy	Electricity, district heating and cooling, oil, gas, hydrogen
Transport	Air, rail, water, road transport	Transport	Air, rail, water, road transport
Banking	-	Banking	-
Financial Market Structures	-	Financial Market infrastructures	
Health	Health care settings	Health	-
Drinking water supply and distribution	-	Drinking water	-
-	-	Waste water	-
Digital infrastructure	Types: IXPs, DNS service providers, TLD name registries	Digital infrastructure	Types of entities: cloud service providers, data centres, etc.
		ICT-service management (B2B)	-
-	-	Public administration entities, excluding the judiciary, parliaments and central banks	-
-	-	Space	-

Table 3: OES in NIS1 and sectors of high criticality in NIS2

The second group of entities subject to obligations under NIS1 is digital services. This is however abolished under NIS2. Important entities in NIS2 include some types of digital service providers,[26] but also a considerable number of new sectors fall under the scope of the concept, and thus are subject to the obligations and requirements of the revised Directive.

NIS1	NIS2
Types of digital services	Other critical sectors (Annex II NIS2)
Online marketplace	Postal and courier services
Online search engine	Waste management
Cloud computing service	Manufacture, production, and distribution of chemicals
	Food production, processing, and distribution
	Manufacturing
	Digital providers
	Research

Table 4: Digital services v critical sectors in Annex II NIS2

While the Commission Proposal had made a distinction between Annex I being essential entities and Annex II important entities,[27] the political agreement text of NIS2 added a size component to the qualification of an essential or an important entity. More specifically, Annex I provides sectors of high criticality, while Annex II other critical sectors. Entities in Annex I (Table 3, right column)

[25] 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.

[26] Cloud computing services are however now part of essential entities as 'digital infrastructure.'

[27] COM (2020) 823 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0823&from=EN, Accessed 8 July 2022.

are essential entities when they exceed the ceiling of a medium-sized enterprise. In case the entities of Annex I NIS2 are medium sized enterprises, then they are considered important entities (Art. 2a (1) NIS2).

Further, Article 2(1) provides the following entities as being always essential entities:

- qualified trust providers, top-level domain name registries, and DNS service providers
- providers of public electronic communications networks or publicly available electronic communications services (meeting, but not exceeding the ceiling of medium-sized enterprises)
- public administration entities of central governments and at regional level (art. 2(2a) NIS2)
- critical entities in the meaning of the (new) Resilience of Critical Entities Directive
- OES identified by Member States under NIS1 or national law

Member States may deviate from the rule of Art. 2a(1) NIS2, and on the basis of national risk assessments establish any of the entities listed in Annex I and II as essential.[28]

In general, all the entities in Annexes I and II that do not qualify as 'essential', they are considered 'important'.[29]

When the above categories of essential and important entities are micro and small enterprises, they are in principle exempt from the applicability of the NIS2 and its obligations.[30] However, this rule is subject to exceptions (Art. 2(2) NIS2). For example, providers of public electronic communications networks or publicly available electronic communications services, trust service providers, and top–level domain name registries and domain name system, are subject to NIS2. Public administrator entities of central governments, and public administration entities at regional level[31] are also subject to NIS2.

Furthermore, the NIS2 establishes requirements for cybersecurity risk management. Those include reporting obligations for incidents with significant impact and other incidents. Essential and important entities are obliged to take proportionate and appropriate measures against risks associated with the security of network and information systems (Art. 18(1) NIS2). These organisational, operational, and technical measures range from risk assessments and information system security policies to the use of encryption (Art. 18(2) NIS2). Compliance with these required measures must be demonstrated by these entities (Art. 17 NIS2). As per the reporting obligations, essential and important entities should notify competent authorities or the CSIRT of significant incidents without delay (Art. 20 (1) NIS2). The criteria to determine the significance of an incident are provided for in NIS2: Incidents are significant if they have the potential to cause substantial operational disruption or financial loss to the entity and the incident has the potential to cause material and non-material losses to natural or legal persons (Art. 20 (3 and 4) NIS2). Significant incidents, cyberthreats, and near misses may also be reported voluntarily by entities that fall outside the scope of the Directive. (Art. 27(1)(b) NIS2). Essential and important entities may report on a voluntary basis the cyberthreats, near misses, and other relevant incidents that do not qualify as 'significant' (Art. 27(1)(a) NIS2).

Member States may choose to make mandatory the use of certified ICT products, processes,

[28] This is possible if the criteria of Article 2(2)(c) to (f) are met, according to Article 2a(1)(d).

[29] Art. 2a(2) NIS2.

[30] Art. 2(1) NIS2.

[31] Public administrator entities in public security, law enforcement, defence or national security are excluded (Art. 2(3)(a) NIS2), unless Member States decide differently (Art. 2(3)(b)NIS2).

and services (Art. 21 NIS2). As in NIS1, following technology-neutral European or internationally accepted technical standards and specifications are encouraged (Art. 22 NIS2) and can be used for the purpose of the reporting obligations and databases of domain names and registration data should be established by the Member States (Art. 23 NIS2).

In addition, NIS2 requires that Member States allow essential, important, but also other entities, which are not in the scope of the Directive, to share information with each other in the form of communities of essential and important entities (Art. 26 NIS2). This information relates to, for example, cyber risks and sensitivities (Art. 26(1) NIS2). The purpose of this information sharing is to better cope with incidents and to strengthen the level of cyber security (Art. 26(1) NIS2).

As regards jurisdiction, the entities belong to the jurisdiction of their establishment in principle (Art. 24(1) NIS2). Exceptions apply to 1. providers of public electronic communications networks or providers of electronic communications services, who belong to the jurisdiction of the Member State where they provide their services (Art. 24(1)(a) NIS2), 2. DNS services providers, cloud computing service providers, data centre service providers, and others (points 6, 8 and 8a of Annex 1 NIS2), which belong to the jurisdiction of the Member State in which they have their main establishment in the Union, (Art. 24(1)(b) NIS2) and 3. public administration entities, which belong to the jurisdiction of the Member State, which established them (Art. 24(1)(c) NIS2). In case the entity has no establishment in the European Union, but offers services within the Union, a representative must be appointed (Art.24(3) NIS2).

The sixth chapter of the NIS2 Directive deals with supervision and enforcement. Member States must ensure that competent authorities monitor and take measures to ensure compliance with the obligations of the Directive (Art. 28(1) NIS2). In doing so, authorities may adopt a risk-based approach in prioritising their tasks (Art. 28(1a) NIS2).

With regard to supervision and enforcement measures, a distinction is made between essential entities (Art. 29 NIS2) and important entities (Art. 30 NIS2). The competent authorities should have at their disposal a wide range of supervision measures for essential entities, such as regular security audits (Art. 29(2) & 30(2) NIS2), and enforcement measures, such as the issuing of binding instructions (Art. 29(4) & 30(4) NIS2). When taking measures, several (listed) factors must always be considered, such as the seriousness of the infringement and the importance of the provisions breached (Art. 29(7) & 30(5) NIS2).

The authorities must also be able to impose administrative fines (Art. 31 NIS2). These must be effective, proportionate, and dissuasive (Art. 31(1) NIS2) and may be imposed in addition to any other measures (Art. 31(2) NIS2). If there is a personal data breach, the procedure of Article 33 of the General Data Protection Regulation should be followed (Art. 32(1) NIS2). In such a case, there is only one way to impose an administrative fine (Art. 32(2) NIS2).

Moreover, within 24 months of the introduction of NIS2, Member States should introduce penalties into national legislation (Art. 33 NIS2). Finally, the authorities of the different Member States should engage in mutual assistance with each other when necessary (Art. 34 NIS2).

4. Comparative analysis of CSIRT tasks under NIS1 and NIS2

The impact assessment study for the legal reform of the Network and Information Security Directive showed that the broadening of the scope of the Directive (as proposed by the European Commission) and the expansion of tasks of national authorities, would mean an increase of 20-30% of resources, including staff, of the relevant authorities per Member State mainly to:

- Perform supervision tasks on a larger number of entities, and
- Interactions with the industry and different sectors.

Specifically for incident reporting, the Commission estimated an approximate increase of 10-15% in the staff tasked to handle incident reporting.[32]

This section offers 1) a comparative overview of the changes to the main capabilities and tasks of CSIRTs (see also Annex 1) and 2) a brief analysis of the CVD and Proactive scanning tasks.

4.1 Organisation, capabilities, and requirements of CSIRTs

NIS2 provides in Art. 9(1) the obligation of Member States to designate one or more CSIRTs. As a whole, the CSIRTs designated in a given country need to cover all the sectors and subsectors of essential and important entities. A CSIRT may be established, within a competent authority, but not necessarily. The EU legislator recognises that co-locating a CSIRT in the supervisory authority may impact the trust relationship between constituencies and the CSIRT. For that reason, it is recommended to design "a functional separation between the operational tasks provided by CSIRTs, notably in relation to information sharing and support to the entities, and the supervisory activities of competent authorities" (Recital 24 NIS2). Next to infrastructure, the staff should be well-equipped and abide by confidentiality and trustworthiness principles (Rec. 35bNIS2).

Member States carry several obligations when it comes to ensuring that CSIRTs are prepared to perform their tasks. Those MS obligations concern both making sure that *each* CSIRT has the necessary infrastructure and secure information sharing tools are in place (Art. 9(3) NIS2). In fact, if possible, Member States should strive to ensure an equal level of technical capabilities for all sectorial CSIRTs (Recital 25 NIS2). Further, Member States should also ensure cooperation of CSIRTs in the CSIRTs Network, in an effective, efficient, and secure manner (Art. 9(6) NIS2).

The requirements for an entity to qualify to be designated as a CSIRT to the European Commission, are similar to those of Annex I of NIS1, but they are more specific and more demanding. Requirements for high level of availability of communication channels, supporting information systems in secure sites, adequate staffing to ensure availability of services at all times, a system for managing and routing requests, and the possibility to participate to international cooperation networks (Art. 10(1) NIS2) were already part of NIS1, even though in an Annex. New added requirements and capabilities for CSIRTs include:

- A **transparency obligation** to clearly specify and communicate to the consistuency and other cooperation partners the CSIRTs communication channels (Art. 10(1)(a))
- A **confidentiality and trustworthiness** of operations obligation (Art. 10(1) (ca))

[32] European Commission, 'Commission staff working document – Impact Assessment Report – Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', SWD (2020) 345 final, 84.

- **Appropriate training** of the CSIRT staff (Art. 10(1)(d))
- A **business continuity obligation** by being equipped with redundant systems and back-up working space (Art. 10(1)(e)).

4.2 Tasks and powers

The tasks and powers of CSIRTs have been substantially amended in NIS2. CSIRTs play a more central and pivotal role than before, by taking on new roles and expanding old ones under NIS1.

Art. 9(1) provides that CSIRTs should be responsible for incident handling, on the basis of a well-defined process. Thus, the core activity of CSIRTs remains incident handling, where handling refers to "all actions and procedures aiming at prevention, detection, analysis, and containment of, response to, and recovery from an incident" (Art. 4(6) NIS2). Responding to incidents, but also – where applicable - providing assistance to concerned entities (Art. 10 (2)(c)). In general, CSIRTs are tasked to monitor and analyse cyberthreats and vulnerabilities, next to incidents. While NIS1 provided that CSIRTs could only do monitoring and analysis of incidents, , NIS2 expanded both the material scope of this task. Upon request, CSIRTs also provide support to entities "regarding real-time or near real-time monitoring of their networks and information systems" (Art. 10(2)(a) NIS2). Furthermore, CSIRTs are tasked to collect and analyse forensic data but also to provide risk and incident analysis. This task will be particularly helpful for victims, that do not have internally or in another way the capacity to conduct such an analysis themselves.

Within the information sharing task of providing early warnings, alerts, and other information on cyber threats, vulnerabilities and incidents to entities regulated in NIS2, Art. 10(2)(b) provides that CSIRTs should provide such information also to "other relevant interested parties". The threshold for this task is quite high, as it is required 'if possible' that the information is shared, 'near-real time.' While NIS2 does not give a clear indication of who those other interested parties may be, those should be differentiated by 'any third parties' and the general public. Paragraph 3 of Art. 10 explains that cooperation relationships of CSIRT maybe be with "relevant actors in the private sector."

In addition, in terms of collaboration, Art. 9(4) NIS2 provides that CSIRTs 'shall cooperate and, where appropriate, exchange relevant information in accordance with Article 26 with trusted sectorial or cross-sectorial communities of essential and important entities.' An important collaboration network is the CSIRTs network (Art. 13 NIS2). According to Art. 10(2)(f) CSIRTs must participate to the CSIRTs network and provide mutual assistance to other members of the network upon their request. The assistance to be provided to other members of the CSIRTs network will be according to capacities and competencies of the CSIRTs, to maintain that CSIRTs may decide on their own, how much effort and resources they may place in the Network. In any case, CSIRTs must participate in the peer reviews of other CSIRTs to be organised in line with Art. 16 NIS2 (Art. 9(5) NIS2)).

As regards cooperation with third countries, the NIS2 provides the option to CSIRTs to collaborate with the national CSIRTs of third countries for information exchange, and collaborate with equivalent to CSIRTs bodies, to provide *them* cybersecurity assistance (Art. 9(6a & b)) NIS2).

4.3 Coordinator of vulnerability disclosure and Proactive scanning

Coordinated Vulnerability Disclosure (CVD) is a new task under NIS2 (Art. 10(2)(fa) NIS2). One CSIRT per Member State is designated as the coordinator of CVD. The coordinator acts as the intermediary between reporting entities and the manufacturers or providers of ICT products or services, that have the vulnerability (Recital 29a NIS2). More specifically, the coordinator CSIRT facilitates the smooth CVD process, supporting entities that report the vulnerability, managing multi-party CVD, in case more entities are affected, negotiates disclosure timelines, and others. In relation to this task, CSIRTs may disclose such vulnerabilities to ENISA's relevant database (Recital 30 NIS2, Art. 6(2) NIS2).

Another newly introduced task in NIS2 is the proactive scanning of networks; private networks upon request of the concerned entity, and public networks at the discretion and will of the CSIRT. In the case of the proactive scanning of private networks, the CSIRT, aims at detecting vulnerabilities with a potential significant impact. Specifically, the competent CSIRT should be able to monitor "the internet-facing assets, both on and off premises" with the aim to discover and manage the "overall organisational risk to newly discovered supply chains compromises or critical vulnerabilities" (Rec. 25a NIS2).

The proactive scanning of public networks on the other hand is aimed at identifying vulnerable or insecurely configured network and information systems, independently of their potential impact. Proactive scanning may offer the power to CSIRTs to have an actual image of vulnerabilities of their constituency, synthesise information into new knowledge, and thus provide more targeted and effective advice and assistance.[33]

At the same time, proactive scanning may be highly intrusive in nature, invading privacy, confidentiality of communications, the protection of personal data, and have a chilling effect on freedom of speech and freedom of expression. This is why, the European Parliament, had initially proposed that the proactive scanning of CSIRTs is limited only to 'serious threats to national security.'[34] Thus, when CSIRTs perform their tasks - especially those that are de facto intrusive by their nature - must conduct an impact analysis and adapt their decision making accordingly. If the risk to violate human rights (and thus act in an illegal manner) is too high, the CSIRT should adopt a less intrusive measure than for instance proactively scanning a network, or at least limit the period and scope of the scanning. Further, CSIRTs should always have a clear framework of operation, setting clear boundaries on what is and what is not allowed by legislation, other than the NIS2, such as a legal basis for processing and human rights impact assessments.

[33] Johannes Wiik and others, 'Effectiveness of Proactive CSIRT Services' (June 2006). < https://www.first.org/resources/papers/conference2006/kossakowski-klaus-papers.pdf> Accessed 27 June 2022.

[34] European Parliament's amended Compromise text to enter the Trialogue negotiations (2021): https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2021/10-28/NIS2_COMPROMISE_amendment_EN.pdf

5. The National Cyber Security Centre the Netherlands: competence and tasks

5.1 Profile – Netherlands

In the Netherlands, the National Cyber Security Centre (Nationaal Cyber Security Centrum; NCSC) performs the CSIRT tasks for vital operators and providers of essential services and serves as the national contact point for cybersecurity notifications, including voluntary notifications. The CSIRT tasks for digital service providers under NIS1 are performed by CSIRT-DSP. The NCSC is a former part of the National Coordinator for Counterterrorism and Security (NCTV) that now operates as an independent entity. The NCTV is still involved in determining the agenda and priorities of the NCSC. Both fall under the responsibility of the Ministry of Justice and Security.[35]

The NCSC fulfils a broad range of tasks related to threat-assessment and incident response. The NCSC does however not operate as the relevant authority that enforces compliance. This is the responsibility of the Telecommunications Agency (Agentschap Telecom; AT) that is part of the Ministry of Economic Affairs and Climate.[36] Under article 4 of the Wet Beveiliging Netwerk- en Informatiesystemen, sectoral responsibility for supervising the compliance of constituents remains with other Ministries or institutions.

The tasks of the NCSC can be divided into three broad categories: the provision of incident response tasks, facilitating and promoting national and international cooperation and operating as an information and knowledge partner. The NCSC is the national CSIRT for providers of essential services.[37] It consists of an (i) operative unit, tasked with incident response, crisis preparation, cyber threat intelligence, technical research and a Fusion Center; (ii) A collaboration and knowledge sharing unit, tasked with relationship management, communication with constituencies, advice and collaboration on the area of cybersecurity, developing knowledge, stimulating scientific research and the dissemination of knowledge; (iii) the technical unit for information provision, tasked with information management, controlling data, project management and development services, and iv) the staff unit on communication, legal advice, management support, and others.[38]

The NCSC has a 24/7 situation centre that can be contacted by its primary constituency: central government, vital operators and providers of essential services. When notifications occur, the NCSC can provide advice, technical analysis, assessments of the quantity of leaked data, use specialized software for logging and combatting malware, provide support the technicians of the constituent, support incident response managers of the constituent, send a response team to the location or activate its international network.[39]

The NCSC promotes national coordination and cooperation, both among public and private institutes.

Nationally, the NCSC plays a central role in the creation of the 'system of national coverage' (Landelijk Dekkend Stelsel; LDS). Here, the NCSC acts as an information hub and partner to entities that help to bolster cybersecurity in the Netherlands. These entities can include

[35] NCTV, 'Organisatie' (2022). <https://www.nctv.nl/organisatie> Accessed 20 June 2022; Organisatiebesluit, Article 54; NCTV, 'Nationaal Crisisplan Digitaal' (February 2020).

[36] NCSC, 'Over het NCSC' (2022). <https://www.ncsc.nl/over-ncsc> Accessed 20 June 2022.

[37] Organisatiebesluit, Article 63h & Wet Beveiliging Netwerk- en Informatiesystemen, Article 3(b).

[38] NCSC, 'Over het NCSC' (2022). <https://www.ncsc.nl/over-ncsc> Accessed 20 June 2022.

[39] *Ibid.*

public entities such as sectoral emergency response teams, Intelligence services (AIVD and MIVD) or private entities that are recognized as important chain organizations (i.e. the Digital Trust Center or Connect2Trust) or that act as parts of Information Sharing and Analysis Centers (ISACs).[40] The Dutch legal and institutional landscape for cybersecurity is set out in-depth *infra* in section 5.2.

Internationally, the NCSC offers the international contact point and represents the Netherlands in the CSIRT network, ENISA, The European Government CERT Group (ECG), Task Force-CSIRT (TF-CSIRT) and the National Liaison Officer Network (NLO Network). As a member of the CSIRT network, the NCSC is tasked with sharing information that is relevant to entities in other Member States of the EU when it involves information on threats or incidents specific to those entities. It is up to the discretion of the NCSC to determine which information can and should be shared in light of cross-border threats or incidents. As a part of the TF-CSIRT, the NCSC may also provide technical or other assistance directly to other Member States if necessary. Outside of these roles of formal representation and response in the European Union, the NCSC also collaborates in the Global Forum on Cybersecurity Expertise (GFCE), Forum of Incident Response and Security Teams (FIRST) and the International Watch and Warning Network (IWWN). Here, the NCSC contributes to the development and dissemination of knowledge and expertise through global cooperation.[41]

Within this network of entities that is involved in bolstering cybersecurity, the NCSC is a vital information partner. The NCSC must determine which information to share with which partners. Here, the NCSC is limited in their ability to share data by legal and practical constraints. Legal constraints arise especially when the information that is to be shared is sensitive or may be used to identify constituents. When information is sensitive, the NCSC must determine if access to this information is vital for receiving entities before sharing it. Aside from sharing information with CERTs or chain organizations, the NCSC can also disseminate non-sensitive or general information to the public.[42]

The upcoming section discusses how different entities shape the legal and institutional cybersecurity landscape in the Netherlands and how these entities in this landscape collaborate with one another, as well as proposals to amend the Wbni to facilitate information sharing.

5.2 Legal and institutional Cybersecurity landscape in the Netherlands

Dutch resilience in the area of cybersecurity is a shared responsibility of the Ministries and the institutions designated by them. These institutions collaborate with one another and organizations in the private sector to ensure a high level of protection in the area of cybersecurity, to prepare for

[40] Cyberwise, 'Infosheet Dutch Cybersecurity Agenda' (2020); WODC, 'Evaluatie van de opbouw en meetbaarheid van de Nederlandse Cybersecurity Agenda' (2021), Final Report. <https://www.dialogic.nl/wp-content/uploads/2020/10/Dialogic-Evaluatie-van-de-Nederlandse-Cybersecurity-Agenda-_Samenvatting_NL.pdf> Accessed 20 June 2022.; Ministry of Justice and Security, 'Beleidsreactie CSBN 2021 en voortgangsrapportage NCSA' (June 2021), Kamerstukken 26 643.; WODC, 'Evaluatie van de opbouw en meetbaarheid van de Nederlandse Cybersecurity Agenda' (2021), Final Report. <https://www.dialogic.nl/wp-content/uploads/2020/10/Dialogic-Evaluatie-van-de-Nederlandse-Cybersecurity-Agenda-_Samenvatting_NL.pdf> Accessed 20 June 2022.

[41] NCSC, 'Over het NCSC' (2022). <https://www.ncsc.nl/over-ncsc> Accessed 20 June 2022.

[42] Ministry of Justice & Security, 'Brief van de Minister van Justitie & Veiligheid aan de Voorzitter van de Tweede Kamer der Staten-Generaal omtrent de verkenning van wettelijke bevoegdheden digitale weerbaarheid en beleidsreacties' (February 2021), Kamerstukken 26 643.

and minimize cybersecurity threats and incidents and to educate and inform companies on best practices.

The Wet Beveiliging Netwerk en Informatiesystemen (Wbni) lies at the heart of the Dutch cybersecurity strategy. The Wbni is the Dutch implementation of the NIS1 and codifies how tasks and responsibilities related to cybersecurity are divided between institutions.[43] Articles 1 and 2 of the Wbni task the Ministry of Justice and Security with the responsibility to set up a national contact point for reporting cybersecurity threats and incidents, to create a CSIRT for suppliers of essential services and to receive voluntary notifications by institutions in accordance with Art. 16 Wbni.

Article 3 Wbni further specifies the tasks of the Ministry, noting the competence of the Ministry to take measures to ensure the continuity of the services offered by vital operators and providers of essential services, the duty to inform these suppliers about threats and incidents and to conduct analyses and technical research in response to cyber incidents or threats that may harm vital operators or providers of essential services. The Ministry has delegated these tasks to the National Cyber Security Center (NCSC)[44] As noted previously, the AT acts as the relevant authority to ensure compliance of vital operators and providers of essential services.[45] The Besluit Beveiliging Netwerk & Informatiesystemen (Bbni) appoints entities as having the status of vital operator or provider of essential services under the Wbni.

Article 3 Wbni stipulates that the Ministry must share information with organisations that have a task to inform the public in this area, the CERTs and internet service providers. Aside from these teams, there are additional cybersecurity CERTs in different sectors.[46]

Sector	Existing CERT in the sector	Governance
Digital Service providers	CSIRT-DSP	CSIRT-DSP Formal CSIRT team, next to NCSC Miinistry of Economic Affairs
Healthcare sector	Z-CERT[47]	Collaboration as a non-for profit foundation of the Dutch Association of University Hospitals, GGZ and The Ministry
Logistics- and waterworks sector	CERT-WM	Rijkswaterstaat in collaboration with waterworks offices

Financial Sector and banking	AAB-GCIRT;
	ING-CERT;
	RaboCSIRT;
		Banks set up their own internal CERTs

[43] 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, OJ L 194, 19.7.2016

[44] the NCSC is tasked under the Ministry with (a) informing, advising and supporting the central government and vital service providers in case of threats or incidents regarding their information systems; (b) informing others about threats and incidents under a; to conduct technical research and analysis for the purpose of fulfilling their tasks under a and b; to inform other parties about the outcomes of this research and analysis; to offer a central contact point as stipulated in the Wbni and to promote private public cooperation.

[45] Besluit aanwijzing toezichthouders Wet beveiliging netwerk- en informatiesystemen [...] energie, digitale infrastructuur en voor digitale diensten 2018.

[46] Other CERTs include ASML-CERT of a large chip manufacturer In the Netherlands (ASML); FoxCERT, T-CERT and RIPE-NCC CERT which offer commercial CERT services and UPC-Chello-security (Ziggo), KPN CERT (KPN) and SIDN CERT (SIDN) which secure the providers of internet networks and other internet services. See Annex 4: CSIRT teams in The Netherlands (source ENISA)p. 59.

[47] See https://www.z-cert.nl/over-ons/ Accessed 20 June 2022.

	PGGM-CERT, and others	
Municipalities	IBD-CERT	Independent entity with a supervisory board where the Dutch Association of Municipalities, large municipalities and the Ministry of Justice are represented.
National Defense	Defense Cyber Security Center[48]	Ministry of Defence
Education & Research	SurfCERT	SurfCERT offers CSIRT services and helps universities to set up their own CSIRTs, these include AMC-CERT), Radboud University (CERT-RU), University of Groningen (CERT-RUG), Utrecht University (CERT-UU), University of Amsterdam (CERT-UVA) and the National Institute for Subatomic Physics (CERT-Nikhef).
Railways	NS-SIRT	Nederlandse Spoorwegen

Table 5 CSIRT-DSP, CERTs and governance

Each of the CERTs above contributes to the cyber-resilience of entities established in the Netherlands, by offering computer emergency response services and/or collaborating with the NCSC. The collaboration between public and private parties as to ensure that each entity in the Netherlands has access to a CSIRT or other cybersecurity provider for emergency response is central to achieving the objectives laid down in the Dutch Cybersecurity Agenda.

The Dutch Cybersecurity Agenda sets out the creation of a 'system of national coverage' (Landelijk Dekkend Stelsel; LDS) as one of its core objectives. The LDS is envisioned as a network where important strategic partners collaborate and exchange information in systematic ways to enhance Dutch Cybersecurity resilience. Collaboration under the LDS happens in several ways.[49]

First, it can either be cooperation between public institutions such as the NCSC, CERTs and the AIVD or MIVD. Cooperation between the AIVD, MIVD and the NCSC happens, *inter alia,* in the National Detection Network (Nationaal Detectie Netwerk; NDN), which also falls within the LDS.[50]

Second, it can be cooperation with public or private 'chain organisations' (schakelorganisaties) such as the Digital Trust Center[51] or other organizations that are made 'Objectively tasked' entities (Objectief Kenbaar Tot Taak; OTTK). Entities can become objectively tasked through Ministerial Decisions that they are chain partners[52]. An OKTT organization does

[48] See https://www.first.org/members/teams/defcert Accessed 20 June 2022.

[49] Cyberwise, 'Infosheet Dutch Cybersecurity Agenda' (2020).

[50] Ministry of Justice and Security, 'Beleidsreactie CSBN 2021 en voortgangsrapportage NCSA' (June 2021), Kamerstukken 26 643.; WODC, 'Evaluatie van de opbouw en meetbaarheid van de Nederlandse Cybersecurity Agenda' (2021), Final Report. <https://www.dialogic.nl/wp-content/uploads/2020/10/Dialogic-Evaluatie-van-de-Nederlandse-Cybersecurity-Agenda-_Samenvatting_NL.pdf> Accessed 20 June 2022.

[51] The Digital Trust Center that is operated by the Ministry of Economic Affairs and Climates informs and educates small- and medium enterprises on how to ensure cybersecurity resilience. Outside of public institutions, there is a variety of private entities that contributes to cybersecurity resilience by collaborating with the aforementioned public institutions as to promote technical knowledge and share best practices.

[52] OKTTs in the Netherlands include the Digital Trust Center (for small- and medium enterprises), Vereniging Abuse Information Exchange (for Dutch internet service providers), Stichting Nationale Beheersorganisatie Internetproviders (for internetproviders and webhosting services), Stichting Cyber Weerbaarheidscentrum Brainport (for the high-tech industry and chain partners), Cyberveilig Nederland (for companies that offer cybersecurity services), Connect2Trust (for multinationals) and FERM (for organisations in the Rotterdam harbour).

not offer emergency response like a CERT, but is instead recognized as an important 'linking organisation' that can receive and disseminate information on potential threats.

Third, ISACs allow for the creation of sectoral collaborations with the involvement of the NCSC or other chain organisations. Within the ISACs, players from certain sectors can exchange information with one another and information partners such as the NCSC or the Digital Trust Center. This promotes resilience, and private entities do not have to fear legal reprisals for potential vulnerabilities as the NCSC is not the responsible authority to check their compliance. Private entities are free to start their own ISACs as to start collaboration, the NCSC or Digital Trust Center will support private entities in the process of developing an ISAC. Private players can also collaborate with one another without involvement of public entities by developing a regional ecosystem of trust or collaborations throughout their supply chain. The NCSC can aid with the establishment of such an ecosystem, but is generally not involved as a partner like in ISACs.[53]

According to policy reports on the progress of the LDS, there have been significant advancements in the creation of the LDS in recent years. Examples of progress in stimulating collaboration are noted as important developments in the Cybersecurity Overview by the Ministry of Justice and Security. Landmarks in creating the Landelijk Dekkend Stelsel include the creation, implementation or expansion of:[54]

- *The Wbni*, which implemented NIS1 and for which proposals exist to amend it as to facilitate information sharing, this is also to be updated when NIS2 is finalized
- *The Digital Trust Center*, which operates as an information partner for small- and medium undertakings in the Netherlands and advises on cybersecurity. The DTC has recently been granted OKTT status and has significantly expanded its collaborations with private entities.[55]
- *The Cyber Intel/Info Cel (CIC),* The Cyber Intel/Info CEL is a cooperation where the NCSC, AIVD, MIVD, public prosecution and the police bring together information into one central physical location to collectively determine risks and threats
- *The CIO platform and risk classification models,* which facilitates the creation of private ecosystems that collaborate to enhance their cybersecurity, for instance by sharing information and experiences[56]
- *Other expansions of the LDS through the creation of more ISACs, appointing more OKTT and involving more supply chain entities as chain organizations*

Other ongoing projects related to the LDS include the creation of a digital platform by the NCSC for the sharing of cybersecurity threats in the energy sector, actualizing the National Crisis Plan

[53] NCSC, 'Aansluiting op het Landelijk Dekkend Stelsel (LDS)' (2022). <https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds#:~:text=Het%20Landelijk%20Dekkend%20Stelsel%20(LDS)%20is%20een%20stelsel%20waarin%20het,en%20kennis%20uit%20te%20wisselen> Accessed 20 June 2022; NCSC, 'Start zelf een samenwerking' (2022). <https://www.ncsc.nl/onderwerpen/start-een-samenwerking/zelf-een-samenwerking-starten> Accessed 20 June 2022. https://www.ncsc.nl/onderwerpen/start-een-samenwerking/zelf-een-samenwerking-starten

[54] Ministry of Justice and Security, 'Beleidsreactie CSBN 2021 en voortgangsrapportage NCSA' (June 2021), *Kamerstukken II,* 26 643.

[55] See NCSC, Aansluiting op het Landelijk Dekkend Stelsel' (2022), https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds, accessed 27 June 2022; Digital Trust Center, ' Digital Trust Center start met actief informeren bedrijven over digitale dreigingen', (2021) https://www.digitaltrustcenter.nl/nieuws/digital-trust-center-start-met-actief-informeren-bedrijven-over-digitale-dreigingen, accessed on 27 June 2022

[56] CIO Platform, 'About Us', (2022), <https://www.cio-platform.nl/en/the-association/about-us> Accessed 24 June 2022.

with respect to cybersecurity and further information sharing possibilities and tools. The NCSC is also actively expanding its collaborations and recent new collaborations include the creation of a circle of trust with multinationals, joining the anti-DDOS coalition and collaborations between the NCSC and Cyberveilig Nederland to create new methods for fully anonymized data sharing.[57]

As the creation of the LDS progresses, the Dutch government tries to identify and resolve any legal or practical barriers that may unduly hinder the collaborative efforts between cybersecurity partners. Per example, the Dutch legislature is currently reforming the Wbni as to resolve the legal barriers which hinder ability of the NCSC and other partners in the LDS. Specifically, the Wbni currently does not include a mechanism for sharing information between the NCSC and important strategic partners that were not designated to have OKTT status.[58]

There is currently a proposal to facilitate the sharing of information more easily and across more instances. If the proposal were accepted as legislation in its current form, it would amend Art. 3 of the Wbni to allow information sharing with a wider range of organisations, including organisations that are not (yet) OKTT entities. This would make it easier to share information across more players within a supply chain and emerging partner organizations to the NCSC. Art.20 of the Wbni would also be amended so that there is no longer the requirement of consent from an organization to share sensitive information related to them with OKTT or CERT entities. Aside from these substantive changes, the proposal also entails changes to the way OKTT organizations are appointed, which would then happen through Ministerial Reglements rather than Minsterial Decisions, in order to align the procedure of appointing OKTT entities and CERTs.[59]

5.3 Changes to the Dutch Cyber security landscape after the introduction of NIS2

The Netherlands is currently preparing for the introduction of the NIS2. The introduction of the revised NIS will significantly expand the constituency of the NCSC, due to the changes described in Section 4. The Netherlands will have to revise both the national transposition law (wbni) and the decree (Bbni).[60]

As identified in a focus group with experts of the NCSC, the agency will need additional human and financial resources to fulfil the increased NIS2 CSIRT tasks, and its own expected revised tasks. From an organisational perspective, the existence of two CSIRTs based on the distinction between operators of essential services – under the NCSC- and the digital service providers -under the CSIRT-DSP – will have to be revisited, due to the revised distinction in NIS2.[61] Some Digital Service Providers are under considered essential and some others important entities. This means that, unless there is a major re-organisation at a national level- a part of the

[57] Ministry of Justice and Security, 'Beleidsreactie CSBN 2021 en voortgangsrapportage NCSA' (June 2021), *Kamerstukken II*, 26 643, Annex 1.
[58] Ministry of Justice and Security, 'Beleidsreactie CSBN 2021 en voortgangsrapportage NCSA' (June 2021), Kamerstukken 26 643.
[59] Ministerial Regulation instead of Ministerial Decree; for the proposal see: Tweede Kamer, Kamerstuk 36084, Wetsvoorstel Wijziging Wet beveiliging netwerk- en informatiesystemen ivm bevoegdheid Minister J&V om dreigings- en incidentinformatie over netwerk- en informatiesystemen van niet-vitale aanbieders te verstrekken aan deze aanbieders en aan OKTT-organisaties (April 2022). <https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A36084> Accessed 22 June 2022.
[60] De Nederlandse Grondwet, 'Herziening richtlijn netwerk- en informatiebeveiliging (NIB-richtlijn)' (2021). <https://www.denederlandsegrondwet.nl/id/vlgnpd2hz1ur/herziening_richtlijn_netwerk_en> Accessed 22 June 2022.
[61] See p. 17 of this Report.

group of previously digital service providers, which will be now considered as essential entities under NIS2, will fall under the responsibility of the NCSC, that is now competent CSIRT for OES. Further, the constituencies in the newly introduced sectors, which are currently not covered by NCSC or the CSIRT-DSP, will have to be assigned to the competence of the existing or a new CSIRT.[62]

The NIS2 – and its implementation into Dutch law through a revision of the Wbni – will impact the legal division of tasks and institutional design in the Netherlands. It will also have a significant practical impact as the scope of regulated entities is broadened, which – if the national division of tasks would be maintained[63] – it would necessitate the NCSC to offer CSIRT services to more undertakings and the national competent authorities (Radio Communications Agency AT, the Dutch Bank DNB, the Inspectorate Healthcare and Youth, Ministry of Infrastructure and Water Management) to supervise more entities.[64] The changes are expected to generate both opportunities and threats, as identified by the focus group with the NCSC-NL and depicted in the table below.

Incident response		
	Opportunities	***Threats***
Organisational	-Reaching out to additional entities significant in the supply chain. -Cooperation with the private sector for support - Visibility of the NCSC's processes -Extension of powers	-Offering sufficient incident response services to the enlarged constituency group -CSIRTs' mandate and service level are not clearly communicated to all constituencies -Applying selectivity to incidents -IT challenges in the context of reporting
Human	- Broader constituency group requires staff with diverse skills: potential for growth of collective skillset -Transparency within the NCSC -Wider network within the NCSC	-Shortage of qualified staff to deal with incident response -No clear guidelines for staff and partners -Knowledge asymmetry between cyber security and target groups -Culture change to tight administration -Recruitment of specialists
Processes	-Visibility of services -Transparency mechanisms -Clearly defined processes	-Gathering sensitive information -Compensate a reduction in trust by transparency mechanisms -IT challenges
Tools	-Automation & standardisation	-Reporting management -Less flexibility & administrative burden
Cooperation and information sharing		
	Opportunities	***Threats***
Organisational	-Standardisation of information sharing	-No existing standards in the transmission of incidents -Focus of NCSC on the national aspect -Information flow between CSIRTs in the EU
Human	-Exchange of outcomes of technical studies -Standardising lists of IP addresses or vulnerabilities	-Member States are focused on their own national target groups

[62] *Ibid.*

[63] See: https://digital-strategy.ec.europa.eu/en/policies/nis-directive-netherlands, Accessed 22 June 2022.

[64] The Fiche predicts an increase in government expenditure of 20-30% compared to government spending on NIS1, see European Commission, 'Impact Assessment Report, Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', *Commission Staff Working Document* of 16 December 2020; see also Werkgroep Beoordeling van Nieuwe Commissievoorstellen, BNC Fiche: Herziening richtlijn netwerk- en informatiebeveiliging (NIB-richtlijn), (online): https://www.europa-nu.nl/id/vlgnpd2hz1ur/herziening_richtlijn_netwerk_en#p1

		-Determining the confidentiality of information is complicated -Contextuality of cases
Processes	-For the operational channels, it is important that the NCSC can also provide consultation -Mandates and legal requirements need to be better mapped	-Undesirable to keep pushing reporting obligations -Complex task to distinguish with whom which type of information can be shared -More complexity & growth of cases
Tools	-Innovation & initiation of the NCSC in order to retrieve information	-Risk of overloading operational channels
Technical research		
	Opportunities	***Threats***
Organisational	-Easier to inform parties -Creating a balance in communication with others	-Capacity issues -The growth in the number of sectors makes it difficult to know all the sectors well -Increased administration could lead to bureaucracy
Human	-Increase of mutual expertise	-Too little attention to ethical challenges
Processes	-Asset management	-Sharing results will require automation as organisations increase
Tools	-Room for automation -Deepening knowledge of specific technical investigations	-Transition period with training of staff for any new tools for automation -More standardisation is required

Table 6: Perceived Opportunities and Threats for CSIRTs under NIS2

6. CSIRTs overview in other Member States

6.1 Overview of Member States' CSIRTs

In this section, a brief overview of the current models and plans under NIS2 and approach of the CSIRTs is presented. The analysis concerns the selected five Member States and is informed by desktop research and the interviews conducted with representatives of CSIRT teams of each Member State.

6.2 Austria

The operation of CSIRT tasks in Austria relies on a private-public cooperation. Firstly, the Office for Strategic Network and Information Security (NIS-Offices) is responsible under the national transposition law of NIS1 (NIS-Gesetz) to perform the strategic tasks attributed to the Federal Chancellery. This includes setting up a connection network between points of contact for the notification of cybersecurity incidents. However, the NIS-Office itself is not the national contact point.[65] The national contact point is operated by the NIS Department of Cybersecurity in the Federal Office for the Protection of the Constitution and Combatting Terrorism. This department is part of the Federal Ministry of Interior.[66]

There are currently the following CSIRT teams: the National CERT (CERT.at), the CERT for public administration offices (GovCERT Austria), which is established within the purview of the Federal Chancellor, and Sectoral CSIRTs (Energy-,[67] Telecommunications-, Aviation CERT). As provided by the national Austrian law implementing the NIS1, the national CSIRT and sector specific CSIRTs support operators of essential services and digital service providers, and the Government Computer Emergency Response Team (GovCERT) supports the entities of public administration, in handling risks, incidents and security incidents.[68]

The national CSIRT is CERT.at is not a public body, but a private entity (*GmbH*)[69] that is accredited as the national CSIRT by the Federal Ministry of Interior. While the national CSIRT determines the need for emergency response, the level of support during incidents is information exchange and coordination, instead of a hands-on approach that would require on-site incident handling for example. CERT.at provides assistance as regards incident triage, incident coordination, incident resolution, and collects statistics about incidents. Further, as regards proactive activities, CERT.at inter alia focuses on collecting contact information of local security teams, distributing knowledge to its constituencies, providing forums for community building and publishes white papers and announcements on security threats to the wider public.[70] In the same line, GovCERT Austria is primarily committed to facilitate information exchange and coordination, but not on-site incident response. GovCERT Austria prioritises incident response on

[65] Bundeskanzelaramt & Bundesministerium Inneres, 'Kontaktstellen von Betreibern wesentlicher Dienste. NIS Fact Sheet 1/2019 – Version 2' (March 2019). < https://www.nis.gv.at/NIS_Fact_Sheet_2019_01_2_0.pdf> Accessed 22 June 2022.

[66] *Ibid.*

[67] Austrian Energy CERT, 'NISG Plattform für Meldungen' (2022). <https://nis.energy-cert.at/> Accessed 22 June 2022.

[68] Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) (2018), Article 14.

[69] CERT.at, 'RFC 2350' (2021). <https://cert.at/en/about-us/rfc2350/> Accessed 22 June 2022.

[70] *Ibid.*

the basis of type and severity of the incident, type of constituency, size and user community affected, and available resources.[71]

As a result of this division of tasks, the CSIRT tasks operated by the CERT.at mostly relate to processing, forwarding information, creating a network of people and organizations and serving as an information hub. The CERT.at determines which notifications need an actual response or which organizations require help in resolving issues related to cybersecurity. The empirical research for this report highlighted that it is often the case that a notification does not require any follow-up response.

The introduction of NIS2 is expected to have impact on the CSIRT teams, but the national CSIRTs already cover all of the constituencies. In view of NIS2, the CSIRTs in Austria need to adapt to the increased tasks and number of entities.

6.3 Denmark

In Denmark, the Danish Center For Cyber Security (CFCS) performs the CSIRT that are normally associated with vital operators and providers of essential services. The CFCS also acts as a national and international contact point. The CFCS is part of the Danish Intelligence Services and falls under the Ministry of Defense. The CFCS consist of several departments:

- one department to perform the CSIRT tasks
- the Net Security Service that monitors the sensor network, the NSS also involves technical research and analysis tasks. [72]
- The department for Civilian Council which provides non-defense related counseling, Defense and accreditation, which develops does defense related counseling and operates as the accreditation body
- the Public Policy department that develops policy and communicates and the Telecommunications Authority that is the relevant authority for cyber security and other public interest tasks.

The CFCS operates a situation center, which is available 24/7. The CFCS looks at the nature of the services provided to see if they are critical, instead of the division between essential and non-essential providers in NIS1. With respect to the CFCS task of operating the national contact point for incidents, Denmark works with a principle of 'sectoral responsibility'. This approach transforms the role of the CFCS to involve more tasks associated with facilitating the sharing of information.

Each Ministry in Denmark has their own area of responsibility (i.e. the Ministry of Energy and Climate is responsible for the energy sector; the Ministry of Public Health is responsible for the health sector etc.). As part of their responsibility, the Ministries are tasked with setting up contact points. the responsibility to develop policy and contact constituencies remains with the relevant authority and their DCIS units, the NCSC only helps in case of emergencies or incidents, but otherwise helps only the services that provide 'critical services.'

These contact points are known as Decentralized Information Security Units (DCIS). These contact points are not CSIRTs and do not perform tasks such as incident response and technical research. However, incidents within certain sectors should first be notified to the Ministry, which

[71] GovCERT Austria, 'GovCERT Austria RFC 2350' (2021). <https://www.govcert.gv.at/2021-03-08_GovCERT_Austria_RFC2350_v1.0.pdf> Accessed 22 June 2022.

[72] Centre for Cyber Security, 'CERT' (2022). <https://www.cfcs.dk/en/about-us/cert/> 27 June 2022.

then communicates it to the CFCS. This means that unlike other Member States, vital operators that fall within these sectors do not contact the CSIRT directly but through their Ministry. While they are not CSIRTS, handling incidents within the sector and developing the maturity of cybersecurity in their sector does remain the responsibility of the Ministry. The CFCS can be consulted by the Ministries and the CFCS can help them when incidents arise.

As regards, information sharing, much of what the CFCS receives will not be published, due to its confidential and sensitive nature, thus sharing of information is only limited. In order to structure information sharing, the CFCS has a platform that allows companies to log in and notify their incidents. That information is then sent both to the relevant DCIS and the CFCS.

In order to facilitate cooperation nationally, the CFCS meets periodically with the DCIS units in their DCIS forum. Here sharing of information takes place and there are efforts to develop processes and foster trust as to build a community of trust that can be expanded with new units under the NIS2. The platform also facilitates voluntary notifications that are sent only to the CFCS. With respect to publishing and sharing the CFCS also looks at the nature of notifications and classifies warnings as general or specific. Specific warnings will not be published and shared with a limited number of entities, while general warnings may be shared with a broader audience. Communications to the public mostly happens through Guidance or Threat Assessments that are published periodically.

The CFCS also stimulates private-public cooperation through several councils and forums. Firstly, the CFCS has created a Strategic Collaboration Forum where cybersecurity experts from public and private institutions talk about strategic efforts. Aside from that, Denmark has a Business Council that represents private institutions with respect to Cybersecurity, a Cybersecurity Council with public and private chairs which discuss policy and strategies. The Cybersecurity Council's public chairs are held by the CFCS and the Digitization Authority, while the private chairs are operated by companies nominated for that task.

Internationally the CFCS cooperates in the CSIRT network, but also in more Defense- or Intelligence related bodies such as NATO. While the NATO related activities cannot be disclosed, the CFCS shares information internationally through the CSIRT network on general matters. When there are incidents that affect other Member States, the CFCS may send a secure email to these Member States' CSIRT to alert them of the threat.

CFCS has been recently re-organised and it is not reported that further significant re-organisation will take place, other than growing in staff. The Danish NCSC intends to explore new methods for public-private collaboration.

6.4 Estonia

In Estonia, CERT-EE is responsible for the provision of CSIRT tasks to vital operators and providers of essential services and for acting as a central point of contact, both nationally and internationally. The CERT-EE is part of the Information Systems Authority (in Estonian: the Riigi Infosüsteem Amet or RIA).

RIA is part of the Estonian Ministry of Economics. The Ministry of Economics has become wholly responsible for cybersecurity past since May 2021. Up until that point, separate departments existed for policymaking and analysis related to cybersecurity as the Ministry was still developing relevant expertise. RIA – as a part of the Ministry - now includes the following departments in their cybersecurity branch. CERT-EE, the Cyber Security Branch are Critical

Information Infrastructure Protection Department, Standards and Supervisory Department and Policy and Analysis Department. RIAs activities are state funded.[73]

The main responsibilities of CERT-EE include dealing with information security incidents within Autonomous Systems AS8240 and AS56588[74], incidents involving vital operators and operators of essential services, providers of telecommunications services, providers of digital services, providers of trust services or other appointed services, as well incidents within most of the state and municipal network that rely on the .ee web domain. Aside from this, the CERT-EE serves as the single point of contact for foreign CERTs and CSIRTs and national CERT, coordinates activities in elevated cases as a part of their threat and incident response duties and commits to national education on cyber security threats and the necessity of arranging cyber security.[75]

There are three pieces of relevant national legislation: (i) the public information act, which ensures that the administration of databases is in accordance with law, other legal acts and proper technical standards; (ii) the emergency act which governs the security and stability of information systems used for the provision of vital services and the permanent implementation of security measures for related information assets and; (iii) the Cybersecurity Act for which the RIA is the relevant authority and it must ensure that there is maintenance of the safety and resiliency of Estonian Information Systems. Constituents can report an incident 24/7 through email or telephone. The CSIRTs incident response team consists of a front office that determines if a notification by a constituent needs to be followed up on. In first instance, reports are categorized between 1 and 6 based on their impact, vulnerability, confidentiality etc.[76] If an incident is deemed critical, a ticket is created through an internal portal through which it will be sent to the back office for technical analysis and to determine which further actions are required in terms of communication to constituents, authorities or the public and to offer assistance and incident response. Once the incident is resolved CERT-EE creates a report on the incident which may include recommendations on how to prevent similar incidents.

Currently, less than 200 entities are part of the CERT-EE constituency. A significant part of the constituency is expected to be under the derogatory grounds laid down in article 2 of the proposed NISD2. While these services would be considered too small in other countries, as they often have under 50 employees, CERT-EE involves them in their constituency on the basis of the critical nature of their services. As a large part of the CERT-EE is already based on national law that offers a higher level of protection than required by the NIS-Directive, the constituency is unlikely to expand significantly. The implementation of NIS2 is expected according to the interviewees for this study, to lead to an increase of a pair of waste management facilities and one or two food production companies.

6.5 France

[73] Republic Of Estonia Information System Authority, 'RFC 2350 Description for CERT-EE' (2020). <https://www.ria.ee/en/cyber-security/cert-ee/rfc-2350.html> Accessed 22 June 2022.

[74] "Autonomous Systems are networks typically governed by large ISPs that participate in global Internet routing. Each network is assigned a unique identification number known as the AS number or ASN by the Internet Assigned Numbers Authority". These AS numbers refer to ISPs serving Estonia's territory; see DBIP Website https://db-ip.com/as56588-information-system-authority Accessed 22 June 2022

[75] *Ibid.*

[76] CERT-EE uses the ENISA guidelines on risk categorization.

The cybersecurity authority in France is Agence nationale de la sécurité des systèmes d'information (ANSSI), which is supervised by the Secretary General for Defence and National Security. France transposed NIS1 in 2018,[77] with the 384/2018 Decree[78]. ANSSI also acts as a Single Point of Contact. In addition to the sectors in the scope of the NIS1 (Annex), the French transposing law includes additional sectors, such as food sector, judicial activities, space and research, several of which are introduced in the scope of NIS2.[79]

The CSIRT tasks are exercised to CERT-FR, which existed before the NIS Directive since 1999. CERT-FR is part of the operational centre of ANSSI and provides support to ministries, authorities, and other public administrative bodies, and also critical infrastructure operators and OES in view of responding to incidents and cyber-attacks.

CERT-FR[80]:

- Detects system vulnerabilities, also through technology monitoring
- Assists in the establishment of means to protection against potential future incidents
- Manages incident responses, with the support of trusted partners, if necessary.
- Fosters and organises a network of trust, with different entities.

CERT-FR provides both reactive and proactive services. Like all CSIRTs, it provides services on a 24/7 basis. In terms of reactive services, CERT-FR provides incident response assistance, support, and remediation, and vulnerability response.[81] In terms of proactive services, CERT-FR provides alerts and warnings, incident analysis and forensics, vulnerability and malware analysis, as well as threat intelligence analysis and sharing.[82] The agency also provides warnings and cybersecurity related news via mailing lists and a web-based portal.[83]

Further, in the framework of cooperation and knowledge sharing, CERT-FR shares Tactics, Techniques, and Procedures, for prevention and reaction purposes. CERT-FR is part of several cooperation exchanging information and feedback.

A prominent public private partnership is InterCERT France, which is a non-for-profit organisation, with the aim to strengthen the capacity of its members to detect and respond to security incidents impacting their environment.[84] Governmental CSIRT information sharing, to which CERT-FR participates are the International Watch and Warning Network (IWWN), and the European Government CERTs Group (EGC).[85]

Under NIS2, in France, there is an expectation of growing of the number of entities, from around 250 currently to around 6000, without calculating the voluntary relations. While ANSSI and CERT-FR do not plan to change their hands-on service of level, there are plans for trusting

[77] Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

[78] Décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

[79] See Chapter 3

[80] CERT-FR, 'À Propos Du CERT-FR' (2022). <https://www.cert.ssi.gouv.fr/a-propos/> Accessed 27 June 2022.

[81] See the cyberthreat landscape 2021 in France: https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf

[82] CERT-FR, 'CERT-FR description – RFC 2350' (2018). <https://www.cert.ssi.gouv.fr/uploads/CERT-FR_RFC2350_EN.pdf> Accessed 22 June 2022.

[83] CERT-FR, 'Alertes de Sécurité' (2022). <https://www.cert.ssi.gouv.fr> Accessed 22 June 2022.

[84] CERT-FR, 'InterCERT France' (2022). <https://www.cert.ssi.gouv.fr/csirt/intercert-en/> Accessed 22 June 2022.

[85] EGC group, 'European Government CERTs (EGC) group' (2022). <https://www.egc-group.org> Accessed 22 June 2022.

and including the ecosystem of cybersecurity actors in the country. Collaboration with private CERTs which are already assisting CERT-FR, will be intensified. To ensure a trusted relationship, ANSSI will continue its qualification and certification programs (ANSSI Security Visa). In 2021 67 qualifications and 88 certifications were already issued under the VISA.[86] Another aspect of trusting the ecosystem is relying on distributed CSIRTs. According to the interviews conducted for this study (April 2022), France is considering relying on intermediaries following a regional and perhaps also sectorial approach.

6.6 Germany

In Germany, the national CSIRT is the CERT-BUND, which is a part of the Federal Office for Information Security (Bundesamt für Sichterheit in der Informationstechnik; BSI). The BSI and CERT-Bund belong to the Federal Ministry of the Interior and Community. The BSI holds the legal mandate under the BSI Act[87], which implements NIS1 in German national law and acts as the Single Point of Contact. CERT-Bund is the section under the BSI that acts as the national CSIRT and provides pro-active and reactive services. Other units within BSI are i.a. responsible for (inter)national cooperation and situational awareness.

In Germany, constituencies that fall within the scope of the BSI Act register themselves with the BSI. Once they are registered, the CERT-Bund may start handling notifications of cyber threats and incidents. CERT-Bund's services are primarily available to the federal authorities, and critical infrastructure.[88] While there are several private CERTs (e.g. the CSIRT for the German Research Network DFN-CERT, or the CERT for the Federal Employment Agency -CERT der Bundesagentur für Arbeit) [89], CERT-Bund is the national CSIRT, and the only German member of the CSIRTs network.

With respect to the process of notifications, German law broadly follows the obligations laid down in Art. 10 NIS1. OES are obligated to report any incident that could eventually result in an outage or disruption of essential services. Reporting occurs through a web-based platform, or by contacting the BSI Control Room that is available 24/7 by telephone or email. After receiving the complaint, sensitive information is anonymized, and the complaint gets processed. Depending on the severity of the incident, CERT-Bund sends information to the victims, has a call with them, or sends a response team to the location of the incident. After the incident has occurred and the initial response has been given, CERT-Bund creates a report which may be public, partially, or wholly confidential. In many instances there are two reports: one confidential and one for the broader public. In terms of tools, CERT-Bund relies not only on the platform for notifications, but also on the Malware Information Sharing Platform (MISP), where known vulnerabilities are logged in a database to ensure responsivity by across the international network.

Information sharing between CERT-Bund and the BSI and other public or private instances mostly happens on the basis of decisions made by humans. However, there are mechanisms that facilitate information sharing. Firstly, standard templates are used for information sharing which

[86] ANSSI, 'Annual Review' (2021). <https://www.ssi.gouv.fr/en/mission/annual-review-2021/> Accessed 27 June 2022.
[87] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) (2009).
[88] BSI Bund, 'RFC 2350', (October 2017). <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KRITIS/rfc2350_CERT-Bund_txt.asc?__blob=publicationFile&v=1> Accessed 22 June 2022.
[89] DFN CERT, 'CSIRT Description for DFN-CERT' (April 2022). <https://www.dfn-cert.de/en/rfc2350.html> Accessed 22 June 2022.

helps the availability of information and clarity on what information to share. Secondly, the UP KRITIS web-based platform allows for information sharing in a more structured way. Access to this platform is voluntary and limited to operators that the state deems critical and sub-threshold operators in essential sectors. BSI supervises that information sharing through this platform happens in the correct way and collaborates with the members of the platform by creating sectoral or thematic working groups. The correct way to share information includes that information is anonymized, that sensitive information is removed and that the sharing is warranted by the nature of the incident. Thirdly, constituents within a critical sector can voluntarily develop ISACs as to share information with one another. The difference between ISACs and UP KRITIS is that the first is only sectoral, while the latter also allows for cross-sectoral and thematic collaboration. Finally, there is the alliance for cybersecurity, where the BSI collaborates with the Federal Association for Information Technology and the Telecommunications and New Media Agency BITKOM. The mission of this collaboration is to strengthen the resilience of German cybersecurity nationwide.

In terms of international cooperation, the CERT-Bund is engaged with the national CSIRTs of other countries, such as Austria, Poland and the Netherlands through bilateral cooperation and information sharing, and also the formal collaboration channels such as the CSIRTs Network. CERT-Bund also contributes to the MISP-platform. To further international collaboration, CERT-Bund has set up mailing and chat programs with other members of the CSIRT network to share information.

Based on an initial guess, the Federal Statistical Office of Germany expects an increase of its constituency to around 45.000 entities under NIS2.[90]

6.7 Remarks

The research has made evident that each Member State maintains its own approach to bolster their cybersecurity and to prepare for the new obligations under NISD2.

Pragmatic approach, coordinator role: The Austrian approach to providing CSIRT tasks under NIS1 was characterized by a pragmatic approach, where the public NIS-office mostly operates as an information hub that facilitated the sharing of information. In preparation for NIS2, the Austrian approach is becoming increasingly hands-on, with more oversight by public authorities.

Distributed responsibility, sectorial approach: Denmark has relied on a sectoral responsibility approach, which relies on the existence of DCIS units to communicate information to the national DCSC, which would in turn decide on a course of action. The DCSC aims to expand this approach while growing in capacity for their national CSIRT department under the DCSC to prepare for a growing constituency.

Centralised, risk-based approach: The risk-based approach in Estonia relies on a highly centralized performance of CSIRT tasks by their CERT-EE. To capture the national situation, CERT-EE provides services beyond what is required of them by NIS1 and is determined to continue to do so under NIS2. They may adjust their risk-based approach to consider not only the importance of the service that is offered, but also prioritize those entities with less in-house technical capabilities.

[90] Interview with BSI and CERT-Bund representatives, April 2022.

Mix of centralised and regional approach: The French 'ecosystem-based' approach, relies on collaborations with trusted public and private partners. These trusted entities - which are either certified or introduced into InterCERT through the proper channels - provide CSIRT tasks while CERT-FR under the ANSSI remains responsible. ANSSI aims to grow and formalize this ecosystem approach and to rely increasingly on automation and standards to adhere to the new responsibilities under NIS2.

Centralised, scalable approach: Finally, the German centralised approach is characterized by the collaboration of Ministries to ensure high responsivity with due attention for differences between sectors. Germany is preparing for the NIS2 by rethinking how they use their tools to ensure their high-quality incident response while scaling up the CERT-Bund to deal with growing constituencies.

In conclusion, each Member State - and their respective CSIRTs and national cybersecurity offices - will have to rethink how their approach to cybersecurity may be impacted by the introduction of NIS2. Problems may arise in terms of capacity, attracting expertise, changing or growing the roles of public and private parties that collaborate with or act as CSIRTs or relying on automation and standards. The transition to new models of organisation may be more or less difficult depending on the current approach and constituency, but CSIRTs are concerned about the long-term impact on their organizational structure and resilience of their national cybersecurity.

7. CSIRTs good practices in selected Member States

This section provides identified good practices in three key areas within the competences of the CSIRTs according to NIS2: incident response, information sharing and collaborations, and technical measures and research. Policy documents and literature follow a similar approach by categorising the good practices themes to capabilities of the CSIRT [mandate capabilities, technical and organisational operational capabilities and co-operational capabilities (ENISA, 2013)], the development and operation cycle of the CSIRT [foundation, establishment, co-operation and trust building, maturity (UN Global Forum on Cyber Expertise, 2017)], (Killcrece, 2004), and the services classification in the RFC 2350 standard [incident response i.e. triage, coordination, resolution, and proactive activities]. [91]

7.1 Theme 1: Incident response

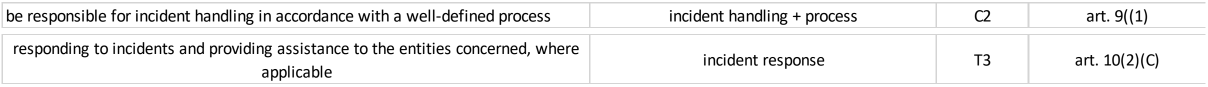
7.1.1 Introduction

Incident response is a key service offered by CSIRTs, as also indicated by their very name. Incident response however is not a mono-dimensional reactive service. Much depends on what CSIRTs consider as 'incident.' The NIS2 (Art. 4(1)(5)) defines as 'incident':

> *"any event compromising the availability, authenticity, integrity, or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems."*

Against this broad definition, CSIRTs need to follow an incident classification system. A prominent example is provided by ENISA, offering a reference for an incident classification taxonomy (ENISA, 2018). [92] Another taxonomy is offered by FIRST, classifying incident per category (e.g. Denial of Service, compromised activity, internal hacking, and others), their sensitivity and criticality.

CSIRTs need to offer services, corresponding to their task in "responding to incidents and providing assistance to the entities concerned, where applicable" (Art. 10(2)(c) NIS2).



be responsible for incident handling in accordance with a well-defined process	incident handling + process	C2	art. 9((1)
responding to incidents and providing assistance to the entities concerned, where applicable	incident response	T3	art. 10(2)(C)

[91] ENISA, 'Good practice guide for CERTs in the area of Industrial Control Systems. Computer Emergency Response Capabilities considerations for ICS' (October 2013). <file:///C:/Users/Gebruiker/Downloads/ICS-CERC%20considerations.pdf> Accessed 22 June 2022; GFCE, 'GFCE Global Good Practices. National Computer Security Incident Response Teams (CSIRTs)' (2017), Conference on Cyber Space 2017. <https://thegfce.org/wp-content/uploads/2020/06/NationalComputerSecurityIncidentResponseTeamsCSIRTs-1.pdf> Accessed 22 June 2022; Georgia Killcrece, 'Steps for Creating National CSIRTs' (August 2004). <https://resources.sei.cmu.edu/asset_files/whitepaper/2004_019_001_53064.pdf> Accessed 22 June 2022; Chris Alberts and others, 'Defining Incident Management Processes for CSIRTs: A Work in Progress' (October 2004). <https://resources.sei.cmu.edu/asset_files/TechnicalReport/2004_005_001_14405.pdf> Accessed 22 June 2022; N. Brownlee & E. Guttman, 'Expectations for Computer Security Incident Response' (June 1998). <https://www.rfc-editor.org/rfc/rfc2350.txt> Accessed 22 June 2022.

[92] ENISA, 'Reference for an Incident Response Taxonomy. Task Force Status and Way Forward' (2018). <https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/@@download/fullReport> Accessed 22 June 2022.

the CSIRT may receive an art. 20 report for incidents having significant impact. the CSIRT may request an intermediate report on relevant status updates by the essential and important entities in line with art. 20(1)	intermediate report request	P1	art. 20 (1)(c)
the CSIRT shall provide without undue delay [..] a response to a notifying entity, including initial feedback and upon request, guidance or other operational advice. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected of criminal nature, the CSIRT shall provide guidance on reporting the incident to the LEAs.	response to incidents with significant impact	T13	art. 20 (5)

Table 7: Selected CSIRT tasks and capabilities for incident response (See Annex)

There are varying services that could be considered as ‘response’ in Incident Response and different service levels to be offered by CSIRTs to their constituencies. The interviewed CSIRTs offer a varying degree of services and mainly service levels, ranging from hands-on approaches (e.g. being ready to offer on-spot incident response services at the location of the victim entity) to more advisory and coordination role of how an incident is handled.

7.1.2 The NCSC-NL situation: a brief overview

At the national CSIRT, the NCSC, incidents are reported via email or by telephone. A template for reporting is also available (see Annex 5). The Incident Response and Forensic Research team is responsible for receiving the reports. Following the reception of the reporting, the Fusion Centre does the triage, reviewing and assessing the reported incident, prioritising. For prioritising, some the first responder assesses questions about the nature and extent of the incident, the possible consequences, the measures already taken and scheduled to be taken by the reporting entity. As regards the level of support offered by NCSC-NL to its constituencies, this is determined as *best effort*, meaning that the NCSC-NL commits to assist to the best of its capacity, but cannot guarantee availability and support to all entities reporting incidents. The support offered by NCSC-NL depends on the type of incident and its severity, as determined the Centre’s first responders. NCSC-NL offers the following services:

Incident response			**Proactive services**
Incident triage	**Incident coordination**	**Incident Resolution**	**Prevention and preparation**
Investigating whether indeed an incident occurred.	Determining the initial cause of the incident.	Providing advice to the reporting party that will help removing the vulnerabilities that caused the incident and securing the systems from the effects of the incidents.	Activities aimed at reducing the probability or impact of an incident for the constituents. NCSC-NL provides the constituents with current information and advise on new threats, and attacks which may have impact on their operations and builds awareness and skills of employees.
Determining the extent of the incident.	Facilitating contact with other sites which may be involved.	Evaluating which actions are most suitable to provide desired results regarding the incident resolution.	
	Communicate with stakeholders and media	Provide assistance in evidence collection and data interpretation when needed.	

Table 8: Overview of reactive and proactive services of NCSC-NL (RFC 2350)

Good practice in the spotlight: The NCSC-NL Fusion Centre

The Fusion Centre can be compared to an incident room, only for digital risks. The centre houses staff with different expertise such as Triage Officers, Signals Specialists, Incident Responders and CTI specialists.
The NCSC therefore takes a broad view of the information that comes from various sources. These include the media, security partners within the government and beyond, target group organisations and other collaboration partners at home and abroad. This enables the NCSC to obtain a full picture of digital threats and to arrive at the necessary insights about an incident or a series of incidents.

Another good practice in NCSC-NL is the open and direct communication with the constituency, and the 'open door policy' within the organisation. As reported in an interview for this project, the NCSC experts try to get involved quickly and help as much as possible.

7.1.3 Good practices from other Member States

A. Service Level in Incident Response in NIS2 and transparency

The practice of MS as regards the provided service level are quite diverse in the interviewed CSIRTs. The service level offered depends on the available resources, the organisational model of cybersecurity and emergency response teams at country level (e.g., hands-on, centralised v. decentralised model, etc.),[93] but also other factors such as culture. CSIRTs, even those that follow a hands-on approach under NIS1, are pragmatic as regards expected service level to their constituencies under NIS2. They show awareness that at least in the initial phase CSIRTs might not be able to treat every incident equally. Some CSIRTs, such as CERT-FR, follow an established incident matrix method, in order to prioritise the handling of the incidents.

Good practice in the spotlight: CERT-FR incident prioritisation method

CERT-FR is using a commitment matrix to assist with the decision-making on how to prioritise incidents according to the available capacity. The matrix comprises of significance of entities (scale A-E) and the risk of the incident (1-5). For example, an A1 incident would trigger national incident response, whereas an E5 would be of lower priority.

Other CSIRTs, such as RIA, follows the ENISA scaling for incidents (ranging from 1 to 6) for incident classification. CSIRTs also have escalation procedures depending on the severity of the event, starting from providing information to the potential victim entity, calling, analysing forensic data from distance, or sending experts on site for support.

Transparency has to do with clear communication from the CSIRTs to the constituency and the broader public of the type and level of offered services, the competence and expertise, the entities under the responsibility of its CSIRT, and other relevant information. As reported in one of the interviews for this study, while voluntary reporting might be less frequent, a motivation for entities to voluntarily notify information in line with Art. 27 NIS2, is the quality of the advice they

[93] See also Chapter 2 of this Report2. Typologies of organisational models and services of CSIRTs.

receive from the CSIRT, as regards handling the incident and additional measures. Thus, transparency about the expected service level, but also quality in the services to be offered, may have a broader impact, than solely the mandatory incident reporting obligations of Art. 20 NIS2.

B. Automation in Incident Response

Due to the expected increase in the reporting of incidents under NIS2, automation in incident response and the degree of desirable automation are recurring questions and objectives. There are several ongoing projects and developed solutions aiming at automating some aspects of incident responding,[94] while other envision a more holistic approach, integrating automation in all aspects of incident response.[95] As a starting point, the majority of the interviewed CSIRTs, and other CSIRTs in the EU, have introduced automation in some stages of incident reporting. Automation aims at eliminating the human involvement and may be introduced in order to:[96]

- Improve efficiency of the IR team
- Improve quality of tasks
- Gathering information, analysing, and providing statistics more easily
- Save resources, especially for repetitive tasks.
- Scalability and predictability.

Automation may take place for example at the level of gathering information (e.g., receiving the reports), analysis, responding, conducting forensic investigations.[97] Commonly automation is categorised in robotic process and cognitive automation.[98] Robotic process automation (RPA) concern types of processes such as alert monitoring, while cognitive automation involves machine learning to improve responses on cyberthreats.[99] However, there are several risks lying with an increased degree of automation, such as for example that if automation tools are not continuously updated or patched, they are too subject to attacks, or the level of performance and errors.[100] In all, when considering to introduce automation in any aspect of incident response, CSIRTs should strive to achieve a good balance between automation and human decision-making. Automation is mostly suited for repetitive tasks to avoid duplication of work, while cognitive automation is mostly useful for statistics, analytics, and correlations, after the incident handling has taken place. In any case, human oversight and decision-making should not be replaced by automation, since every incident has its own unique characteristics.

[94] See Incident Handling Automation Project: https://github.com/certtools/intelmq; https://intelmq.readthedocs.io/en/latest/user/ecosystem.html Accessed 22 June 2022

[95] See for example Public-Private Partnership Automation of Security Operations, Technical Execution Program, TNO (2020) https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/trusted-ict/cybersecurity/automated-security/; https://www.euractiv.com/section/cybersecurity/news/france-launches-new-cyber-campus-to-boost-cybersecurity-strategy/ Accessed 22 June 2022

[96] Alexandre Dulaunoy, 'CTI and Automation. Supporting CSIRT capabilities and reduce manual operations', presentation CTI-EU event (2020). <https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/supporting-csirt-capabilities-and-reduce-manual-operations/> Accessed 27 June 2022.

[97] Threat Intelligence, 'Automated Incident Reponse: What It Is, Tools and Use Cases (*Threat Intelligence*, 23 August 2021). <https://www.threatintelligence.com/blog/automated-incident-response> Accessed 27 June 2022.

[98] Lacity M and L Willcocks, *Robotic process and cognitive automation: the next phase* (SB Publishing 2018).

[99] L Pitt, 'Security Automation Challenges to Adoption: Overcoming Preliminary Obstacles' (*Securityweek*, 10 July 2020) <https://www.securityweek.com/security-automation-challenges-adoption-overcoming-preliminary-obstacles> Accessed 27 June 2022.

[100] Onwubiko C, 'CyberOps: Situational Awareness in Cybersecurity Operations' (2022), Vol. 5, International Journal on Cyber Situational Awareness.

C. Making use of the cybersecurity ecosystem

Next to any internal training programs, some countries such as France have plans for an active engagement with the cybersecurity ecosystem of the country. This involves, among others, making use of the services of private consultants. To ensure the reliability, independence, and expertise of the consultants, ANSSI runs a certification program. Similarly, BSI also provides certifications of persons on the basis of the Act on the Federal Office for Information Security (BSI Act). Qualified persons are required to perform evaluations and tests for the purpose of certifying products and management systems, as well as to support the BSI in IT security services. The aim of the procedure is to provide competent persons in the areas of application and to ensure the quality and comparability of the evaluations/examinations, audits, and services. This practice is quite common in other countries too, such as for example the UK and its national CSIRT, the NCSC-UK, which provides a certification program for Cyber Incident Response services, but also Proactive security event discovery, Response, and recovery planning services.[101] Next to services, the NCSC-UK provides professional skills and training for individual experts (Certified Cyber Professional – CCP).[102] Certification programs are policy instruments to increase the overall resilience of the cybersecurity products, systems, processes, and services.[103]

Good practice in the spotlight: The ANSSI Security VISA[104]

The ANSSI Security VISA is a mark of credibility and an important asset for companies. It is a recognition of the level of cybersecurity of a product or a service. It includes three types of objectives: regulatory, contractual, and commercial. The ANSSI Security VISA is now available to entities established in France, but it could potentially be adapted to be a pan-European type of certification.

However, in a large crisis, large IT-security providers are bound to offer their services to entities with which they have contractual arrangements, and no other victims – re-directed or recommended by the national CSIRT for example- that do not have such contracts yet.

Good practice in the spotlight: BSI's volunteer Cybersecurity Network program

BSI is running a pilot phase of a volunteer program with people that are not IT-professionals, but willing and prepared to act like a 'fire-brigade' to help smaller companies in the scope of NIS2. Those professionals have to pre-qualify for a training program, which may lead to personal certification by BSI, and will offer their services for a fee to victims, upon request.

[101] National Cyber Security Centre, 'CNI Hub' (2022). <https://www.ncsc.gov.uk/section/private-sector-cni/products-services> Accessed 27 June 2022.
[102] National Cyber Security Centre, 'Certified Cyber professional (CCP) assured service' (2018). <https://www.ncsc.gov.uk/information/certified-cyber-professional-assured-service> Accessed 27 June 2022.
[103] Weiss M and Biermann F, 'Cyberspace and the protection of critical national infrastructure' (2021), Journal of Economic Policy Reform; Kamara and others, 'The cybersecurity certification landscape in the Netherlands after the Union Cybersecurity Act', National Cybersecurity Centre (2020).
[104] ANSSI, 'The ANSSI Security Visa by the French National Cybersecurity Agency' (2022). <https://www.ssi.gouv.fr/en/actualite/the-anssi-security-visa-by-the-french-national-cybersecurity-agency/> Accessed 27 June 2022.

Another means to engage and leverage the expertise and know-how of the private sector, is through Public-Private Partnerships, as explained in the following section. In brief, as also Recital 26g NIS2 encourages, through PPPs the community can benefit from state-of-the art services and processes such as in:

- information exchange
- early warnings
- cyber threat and incident exercises,
- crisis management, and
- resilience planning

An innovative approach of making use of a country's cybersecurity ecosystem, is the French Cyber Campus, combining different actors of the cybersecurity ecosystem in one physical location.

Good practice in the spotlight: The French Cyber Campus[105]

The Cyber Campus is a common physical location, where representatives of the whole cybersecurity ecosystem of the country e.g. start-ips, SMEs, private cybersecurity specialists, researchers, labs, governmental departments, training organisations, users, and others, work together, liaise and collaborate, to enhance cybersecurity in France and beyond.
The aim is the Cyber Campus becomes a centre of gravity for cybersecurity and digital trust. The Campus received public funding for its launch phase but is expected to be self-financed from its members and have its own legal personality.

D. Upscaling staffing capacity with training program

While CSIRTs are aware of the need for increased staff, they cannot always in short-term recruit new personnel. One reason is the need for security clearances, which are necessary to work at a national CSIRT for example. Especially in CSIRTs that are part or otherwise related to foreign intelligence offices and/or a ministry of defence, this process can be quite lengthy and not linear. A second reason has to do with the available skills and training. In smaller countries, it is reported that cybersecurity experts are often absorbed by the private sector, which might offer more attractive payments. To address this issue, CSIRTs are developing or intensifying training programs:

- **At post-secondary/advanced education**, which ensures a stable stream of incoming or available personnel. On the downside, this practice does not ensure very highly skilled personnel directly and it requires time and resources investment for the CSIRTs.
- **As internal training of personnel** that wishes to move horizontally from their current position towards Incident response or collaborations and partnerships. This practice works better CSIRTs that are already a large organisation (so that they horizontal mobility

[105] Michel van den Berghe, 'Cyber Campus. Uniting and Expanding the Cybersecurity Ecosystem' (2020). <https://www.ssi.gouv.fr/uploads/2019/10/campuscyber-rapport-en.pdf> Accessed 27 June 2022.

would not create a new gap) or part of larger organisations (e.g. CERT-Bund is part of BSI in Germany).

- **Training of employees of essential entities,** which increases the awareness and expertise of the constituencies. (e.g. L'Observatoire des métiers de la cybersécurité).[106]

Good practice in the spotlight: The Danish Cybersecurity Academy

The Danish Centre for Cyber Security has focused on the development of competences in specific areas. To that end, the Danish Cybersecurity Academy, trains junior analysts, right after secondary education.

Another reported way to address part of the scarcity of available experts, to appoint less-experienced employees in the front office to do the triage, while the more experienced experts conduct the technical analysis.

E. Ensuring accuracy of information

Accuracy of the information is pivotal. CSIRTs would need to make sure that facts instead of speculations are reported. While the process cannot be automated, one way put forward by interviewees, to ensure the quality and accuracy of information, is placing some responsibility on the reporting entities. This responsibility could take the form of a legal obligation in the national law transposing NIS2. While there is already the legal obligation under data protection legislation (principle of accuracy under (5(1)(d) General Data Protection Regulation), this is not sufficient, since the information provided by a reporting entity is not exclusively personal data. However, it is also important to not over-penalise entities for not sharing accurate information, as much information about an ongoing incident, might be available only months after the incident took place. A qualification of the responsibility to share accurate information to 'the best of knowledge' of the reporting entity and/or without intention to misguide the CSIRT could address the risk of over-penalisation.

7.2 Theme 2: International and national cooperation

7.2.1 Introduction

International and national cooperation for information sharing and operational support, where feasible, is a very important aspect of the CSIRTs tasks. This is apparent from the CSIRTs tasks in NIS2, that emphasise the importance of a community of sharing knowledge and information. A common ongoing practice among CSIRTs is to contact "colleagues from other CSIRTs with whom they had previous contact and whom they know personally."[107] While this practice continues, it is foreseeable that in view of the growing number of CSIRTs and constituencies under NIS2, it will become eventually more challenging to maintain trust on the basis of a prior personal contact. The

[106] ANSSI, 'Observatoires des Métiers de la Cybersécurité' (2022). <https://www.ssi.gouv.fr/particulier/formations/observatoire-des-metiers-de-la-cybersecurite/> Accessed 27 June 2022.

[107] Van der Meulen N, 'Stepping out of the Shadow: Computer Security Incident Response Teams in the Cybersecurity Ecosystem' (2021), The Oxford Handbook of Cyber Security, 297.

capability of a CSIRT to participate in cooperation relationships and cooperation networks is one of the mandatory requirements for designating a computer emergency response team as a CSIRT in line with Arts. 9 and 10 NIS2.

have the possibility to participate in intenational cooperation networks	participation to international networks	R7	art.10 (1)(f)
cooperate and exchange information with trusted sectorial or cross-sectorial communities of essential and important entities	cooperation and information exchange consistuencies	C3	art. 9(4)
May establish cooperation relationships with national CSIRTs of third countries	3rd country cooperation with national CSIRTs	C5	art. 9(6a)
May cooperate with CSIRTs or equivalent bodies in third countires, to provide them with cyversecurity assistance	3rd country CSIRT for cybersecurity assistance	C6	art. 9(6b)
participating in the CSIRTs network and providing mutual assistance according to their capacities and competencies to other members of the network upon their request.	CSIRTs network members support	T7	art. 10(2)(f)
CSIRTs shall establish cooperation relationships with relevant actors in the private sector, with a view to better achieving the objectives of the Directive	cooperation with private actors	T10	art. 10 (3)
Where they are separate, the competent authorities referred to in Article 8, the single point of contact and the CSIRT(s) of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive	national cooperation	T11	art. 11
Participate in Art. 16 peer-reviews	peer review	C4	art. 9(5)

Table 9 Selected CSIRT tasks and capabilities for cooperation (See Annex)

7.2.2 The NCSC-NL Situation: a brief overview

In terms of national cooperation, the Netherlands pursues a strategy to create a 'system of national coverage', which is characterized by collaboration between public and private parties that may be CSIRTs, OKTT entities or private entities that aim to promote general or private interests. Sharing information via sectoral ISACs is reported to be beneficial in the Netherlands, especially as regards sharing best practices in cybersecurity incident handling.[108]

Good practice in the spotlight:
The Dutch System of National Coverage (LDS)

The Netherlands has chosen to converge public and private interests into a system where different entities can collaborate as a part of their own private ecosystem, as part of an ISAC, as a 'chain organization' in terms of computer emergency response and monitoring or as a public or private party that is involved laterally (for instance the AIVD or the MIVD, or providers of important technologies such as ASML). These collaborations are captured and formalized in the system of national coverage, known as the Landelijk Dekkend Stelsel or LDS.[109]

The Dutch Cybersecurity Agenda aims to ensure that every entity in the Netherlands - whether vital or essential or not - has access to a provider of CSIRT tasks and adequate aid in maintaining a high level of cybersecurity resilience. This complex web of formal and informal

[108] Bekkers L. et al, Verkenning best Practices cybersecurity Informatiedeling (2020) https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/rapport-a4-lectoraat-cybersecurity-in-het-mkb.pdf
[109] See also: Changes to the Dutch Cyber security landscape after the introduction of NIS2 23

collaborations and cooperation can entail anything from information sharing on threats or incidents, learning about best practices, or aiding in emergency response.[110] As regards partnerships and collaborations at European and international level, NCSC-NL is very well merged in recognised information sharing networks and communities. NCSC-NL uses Traffic Light Protocol to signal the sensitivity of the information, and shares information following a "Need to know" principle.[111]

> Good practice in the spotlight:
> The NCSC Cyber Compass for the wider public
>
> In order to assist organisations to remain resilient and anticipate changes as regards cybersecurity, the NCSC publishes on its website guidance, written in simple terms for non-expert audience.
> The Cyber Compass provides foresight insights for 8 aspects of cybersecurity: 1. Digitalisation 2. Increase in legislation and regulations 3. Intelligent mobility 4. Homogenisation of the digital landscape 5. Monopolisation of the digital domain 6. Increased incident response complexity 7. Decline of the human factor 8. Reduced freedom to choose suppliers.
> →Updating the Cyber Compass at a more regular basis with information for example on the changes for constituencies under the scope of NIS2, the new reporting obligations and voluntary notifications, as well as cybersecurity risk management would be a useful starting point for many entities established in the Netherlands.

7.2.3 Good practices from other Member States

A. Confidentiality of information and means to ensure it

Interviewed CSIRTs take confidentiality of information very seriously. Information that is confidential is treated with care, so that only the relevant entities will have access to only the necessary information. One good practice is to draft two types of incident reports; an internal report with confidential information, and a public one sharing only what is necessary for a broader audience.

> Good practice in the spotlight: Anonymisation
>
> Anonymisation of sensitive information that is shared with different actors (authorities, essential or important entities, etc.) is seen as a good practice, which fosters trust from the constituencies towards the CSIRTs.
> It should also be noted that anonymisation has limitations on how effective it is, especially when a shared incident is taking place in a smaller country, or it concerns a large entity or provider.

[110] See also: Profile – Netherlands, p. 24

[111] Nationaal Cyber Security Centrum, 'Het Traffic Light Protocol' (2022). <https://www.ncsc.nl/onderwerpen/traffic-light-protocol> Accessed 27 June 2022.

In the same vein, CSIRTs aim not at top-down communication and hierarchical relationship, but a trusting relationship with their constituencies. This also incentivises voluntary notification of events, in the absence of a relevant obligation.

B. Information sharing – with whom and how

There are several ways to share information with constituencies, authorities, and other Art. 9(4) NIS2 already points at both sectoral and cross-sectoral communities of essential and important entities. Many of the interviewed countries rely on Public-Private Partnerships in the form of Information Sharing and Analysis Centres (ISAC) for the sectorial information sharing. In fact, Recital 26g NIS2 encourages PPPs for 'knowledge exchange, sharing of best practices, and the establishment of a common level of understanding' for cybersecurity stakeholders,
The information shared at ISACs is usually technical and tactical,[112] but depending on the specific ISAC there might also be a practice developed and agreement for sharing other types of information.[113] The cross-sectoral communities may be organised around:

- *Thematic focus* such as malware, independent of sectors or type of entity (essential or important).
- *Supply chain actors*. The importance of protecting the whole supply chain is highlighted with several obligations in NIS2, such as the Art. 18(2)(d) NIS2) which introduces a mandatory measure for essential and important entities for supply chain security, including aspects of the relationships between each entity and its direct suppliers or service providers.
- *Governmental and public administration* CERTs.
- Other.

In order to maintain trust among members of the various information sharing networks, a good practice is approval by (voting or recommendation) from existing members. Next to membership requirements, smaller working groups, can create circles of trust, which decide what information to share with the other members of the community.

Information sharing should also take place to the correct audience first to avoid notification fatigue of the constituencies, and second to ensure that sensitive information is communicated to those that will be benefitted from it. A good practice for a CSIRT sharing information with constituencies, self-registration platforms (Germany, Austria).

Good practice in the spotlight:
"Know your constituency platform": self-registration portal

[112] Eric Luiijf and Allard Kernkamp, 'Sharing Cyber Security Information. Good Practice Stemming from the Dutch Public-Private-Participation Approach' (March 2015), Global Conference on Cyber Space 2015. <file:///C:/Users/Gebruiker/Downloads/luiijf-2015-sharing.pdf> Accessed 27 June 2022.
[113] Read further on cooperative models for ISACs: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models.

Austria and CERT.at are developing a "Knowing your constituency" platform, where entities subject to NSI2 will make an account and fill in relevant information. This will take place as self-registration, like a customer portal.

Next to appointing a main contact point for each entity, which is also very important for the continuity of communication beyond personal contacts between the CSIRT and the regulated entity, essential and important entities will also have the option to select the topics they wish to be notified about and the means (via the platform or other means of communication).

In the Danish model of sectorial responsibility, a centralised platform for incident response and information sharing, is also possible. Entities log onto one platform and during the filling in of the form, they are required to indicate their sector. Once filled in, the reporting is directed to both the Centre For Cyber Security as the national contact point, and the sectoral CSIRT. In terms of information sharing, the CFCS distinguishes between general warnings that are sent to entities that signed up for those, and specific warnings that are shared only with relevant parties.

C. Collaboration networks

The following national, European, and international networks are some prominent examples of collaborations for information sharing in terms of technical tooling, information about vulnerabilities, incidents, near misses, and cyber threats. Some of them are thematic (e.g. MISP), some others are actor-oriented (e.g. governmental such as the ECG), but the majority have a broad scope and members (e.g. FIRST). While the list is not exhaustive, those are groups that many of the European CSIRTs participate. The national ones demonstrate the type of existing partnerships and collaborations in some of the interviewed Member States.

A. National

- **UP KRITIS** – is a cross-sectorial Public Private Partnership, between operators of critical infrastructures, their associations and government agencies. UP KRITIS was created for the Implementation of the action Plan for Critical Infrastructure Protection, prepared by the government and the critical infrastructure operators.[114] UP KRITIS aims at increasing the resilience of critical information infrastructures[115] and in specific the focus is on the focus of the work is on the security of IT and OT (Operational Technology, including Industrial Control Systems, ICS) as well as the relevant processes and structures of a functioning ISMS (Information Security Management System). Participants receive situation information and alerts on IT security from the BSI and can exchange information on special incidents as needed within the framework of operational cooperation.
- **Alliance for Cybersecurity** – This is an initiative of the BSI and it has been founded in cooperation with the Federal Association for Information Technology,

[114] UP KRITIS, 'UP KRITIS. Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen' (February 2014). <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/UPK/upk-grundlagen-ziele.pdf?__blob=publicationFile&v=3> Accessed 27 June 2022.

[115] BSI, 'UP KRITIS' (2022). <https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/UP-KRITIS/up-kritis_node.html> Accessed 27 June 2022.

Telecommunications and New Media (BITKOM) in Germany. The aim of the Alliance for Cybersecurity is to increase cybersecurity in Germany and strengthen Germany's resistance to cyber-attacks. Participants receive warnings from BSI, current situation reports, solutions and instructions, and documentation. In principle, any organisation based in Germany can participate. The member sign a confidentiality agreement.[116]

- **InterCERT France** – InterCERT France is an association established under French law, in the responsibility of the Ministry of Defence in France. The purpose of this community is to strengthen each member's ability to detect and respond to security incidents. Participants are CERTs with activity in France, but their activity may extend cross-border, with regard to detection and/or response to security incidents. The permanent members need to self-evaluate their maturity level following SIM3 maturity assessment methodology. Next to permanent members, there are also liaison members.[117]
- **Austrian Trust Circle** – This is a an initiative of CERT.at, in cooperation with Austrian Energy CERT, GovCERT Austria and the Federal Chancellery, which provides a formal framework for practical information exchange and joint projects in the security sector.[118] Its aim is to support organisations, provide operational contacts for CERT.at for information and handling of security incidents, to create a community of trust among its members that can facilitate common incident handling in a case of emergency, and networking and exchange of information.[119]
- **CERT-Verbund Austria** – This is a collaboration community among all Austrian CERTs in the public and the private sector.[120] The aim is joining forces to combine the know-how and promote CERTs best practice activities in Austria.

B. European and International

- **CSIRTs Network –** CNW was created in NIS1 (Art. 1 (1)(c) NIS1) and maintained in NIS2.[121] Its aim is to strengthen the 'confidence and trust and to promote swift and effective operational cooperation among Member States' (Recital 35a, Article 13 NIS2). The Members of the CNW under NIS2 are the representatives of the CSIRTs, which are designated under Art. 9 NIS2.
- **TF-CSIRT- Task force- CSIRT** is a task force that promotes collaboration and coordination between CSIRTs in the EU and neighbouring regions, coordinated by Géant, an association of European National Research and Education Networks. TF-CSIRT aims at safeguarding the maturity process of trusted infrastructure, promote the use of common standards and

[116] BSI, 'Allianz für Cyber-Sicherheit' (2022). <https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html> Accessed 27 June 2022.
[117] CERT-FR. 'Réglement Intérieur InterCERT-France' (2022). <https://www.cert.ssi.gouv.fr/uploads/Réglement_intérieur_InterCERT-France-v1.0.pdf> Accessed 27 June 2022.
[118] Onlinesicherheit.at, 'Austrian Trust Circle (ATC)' (2022). <https://www.onlinesicherheit.gv.at/Services/Initiativen-und-Angebote/Strategische-Infrastrukturen/Austrian-Trust-Circle-ATC.html> Accessed 27 June 2022.
[119] Austian Trust Circle, 'Home' (2022). <https://www.austriantrustcircle.at> Accessed 27 June 2022.
[120] Onlinesicherheit.at, 'CERT-Verbund Austria' (2022). <https://www.onlinesicherheit.gv.at/Themen/Erste-Hilfe/CERTs/CERT-Verbund-Oesterreich.html> Accessed 27 June 2022.
[121] CSIRTs Network, 'CSIRTs Network' (2022). <https://csirtsnetwork.eu> Accessed 27 June 2022.

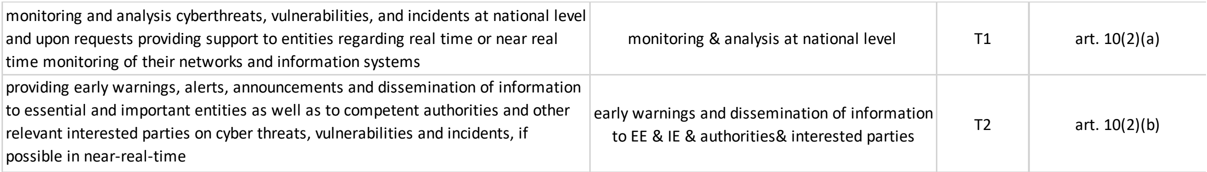
procedures for incident handling, coordinating joint initiatives where feasible, provide training of CSIRT staff ('TRANSITS'). The task force has a partnership with FIRST and ENISA.[122] TF-CSIRT runs a 'Trusted Introducer' program, which provides accreditation and certification services to its members, to ensure a higher level of trust among members.[123]

- **European Government CERTs Group (ECG) –** ECG is an informal operational group focusing on technologies for incident response. Its members are governmental CERTs of European countries.[124]Many of EGC members are members of FIRST and TF-CSIRT.
- **Forum of Incident Response and Security Teams –** First is a non-for-profit organisation, which aims at fostering cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. It has more than 600 members, which are CERTs from governmental, commercial, and educational organisations. There are two categories of membership: full members (with voting rights) and liaison members. FIRST has demanding membership criteria that aim to maintain a trust relationship among its members: new members must be nominated by existing members.[125]
- **International Watch and Warning Network (IWWN) –** This is a global network with representatives of several countries globally, with the aim to safeguard policy and implementation of cybersecurity The IWWN organises exercises, stimulates information sharing and cooperation.[126]

7.3 Theme 3: Technical research and monitoring

7.3.1 Introduction

Technical measures and research, as proactive services or post-mortem analysis of an incident, are a third pillar of the CSIRTs tasks in NIS2. As the NIS2 requires, CSIRTs need to equipped, in terms of staff, tools, and other technical capabilities, to perform their tasks such as collecting and analysing forensic data and providing risk analysis to their constituencies.



monitoring and analysis cyberthreats, vulnerabilities, and incidents at national level and upon requests providing support to entities regarding real time or near real time monitoring of their networks and information systems	monitoring & analysis at national level	T1	art. 10(2)(a)
providing early warnings, alerts, announcements and dissemination of information to essential and important entities as well as to competent authorities and other relevant interested parties on cyber threats, vulnerabilities and incidents, if possible in near-real-time	early warnings and dissemination of information to EE & IE & authorities& interested parties	T2	art. 10(2)(b)

[122] TF-CSIRT, 'TF-CSIRT' (2022). <https://tf-csirt.org/tf-csirt/> Accessed 27 June 2022.
[123] TF-CSIRT Trusted Introducer (2022). <https://www.trusted-introducer.org/processes/accreditation.html> Accessed 27 June 2022.
[124] EGC Group, 'European Government CERTs (EGC) group' (2022). <https://www.egc-group.org> Accessed 27 June 2022.
[125] FIRST, 'FIRST is the global Forum of Incident Response and Security Teams' (2022). <https://www.first.org> Accessed 27 June 2022.
[126] National Cyber Security Centre, 'International coorperation' (2022). <https://english.ncsc.nl/about-the-ncsc/international-coorperation> Accessed 27 June 2022.

collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity	forensic data collection and analysis	T4	art. 10(2)(d)
providing, upon the request of an entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact.	proactive scanning private networks upon request	T5	art. 10(2)(e)
CSIRTs may carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential or important entities. Such scanning shall be carried out to detect vulnerable or insecurely configured network and information systems and inform the entities concerned. Such scanning shall not have any negative impact on the functioning of their services	proactive scanning public networks	T6	art. 10(2)(e)
where applicable, acting as a coordinator for the purpose of the coordinated vulnerability disclosure process pursuant to Article 6 (1) that shall include in particular facilitating the interaction between the reporting entities, the potential vulnerability owner and the manufacturer or provider of ICT products or ICT services in cases where this is necessary, identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure time lines and managing vulnerabilities that affect multiple organisations (multi-party coordinated vulnerability disclosure).	CVD coodinator and management subtasks	T8	art. 10(2)(fa)
contributing to the deployment of secure information sharing tools pursuant to Article 9(3).	secure information sharing tools	T9	art. 10(2)(fb)
CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies for incident handling procedures, cybersecurity crisis management, CVD.	promotion of standardised practices	T12	art 10 (4)

Table 10: Selected CSIRT tasks and capabilities for technical research and monitoring (See Annex)

7.3.2 The NCSC-NL situation: a brief overview

In terms of CVD, NCSC has published dedicated Guidelines, where it provides advice to organisations and delineates the role of NCSC. Even prior to the NIS2 task (T8 – see Table 10: Selected CSIRT tasks and capabilities for technical research and monitoring (See Annex) the NCSC has been voluntarily acting as an intermediary, where the party reporting a vulnerability would not report the vulnerability directly to the organisation or would have had it reported, but the organisation was not responsive.[127] The NCSC also maintains an online form to facilitate such disclosure.[128] The NCSC-NL has not yet a statutory task to perform proactive monitoring of networks.

7.3.3 Good practices from other Member States

A. IT Infrastructure and supporting tools

Investing in IT infrastructure is a priority in CSIRTs following the NIS2 adoption. Only hiring additional staff members is not sufficient. Research has shown that adding more resources to incident handling, will not solve the problem.[129]

Next to infrastructure, tools enable and facilitate the work of CSIRTs. To be able to perform many of their tasks in this category CSIRTs need to ensure they have available the appropriate tools. As ENISA and the SIM3 self-assessment provide, the following are important factors to assess the maturity of a CSIRT, especially one with the increased competences and tasks in NIS2:[130]

[127] National Cyber Security Centre, 'Coordinated Vulnerability Disclosure: the Guideline' (2018). < https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html> Accessed 27 June 2022.

[128] National Cyber Security Centre, 'CVD-report form' (2022). <https://english.ncsc.nl/contact/reporting-a-vulnerability-cvd/cvd-report-form> Accessed 27 June 2022.

[129] Johannes Wiik and others, 'Persistent instabilities in the high-priority incident workload of CSIRTs' (2009), 27th International Conference of the System Dynamics Society.

[130] ENISA, 'SIM3v1 self-assessment tool' (2022). <https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-survey> Accessed 27 June 2022.

1. IT Resources List, that is a list that describes hardware, software and tools of the constituency, and information resources list, where the constituencies receive their information and notifications.
2. Consolidated email system, resilient phone, email and internet access, incident tracking system
3. Incident prevention tools (e.g. IntelMQ), incident detection tools, incident resolution tools.

Two examples in the area of technical measures monitoring come from Denmark and Estonia. It should be noted that those practices are also found suitable for the environment, conditions, and cybersecurity culture of each country. One example is the Danish Net Security Service,[131] in the framework of which "CFCS monitors parts of the networks used by government bodies and critical infrastructure, and is responsible for detecting and analysing threats against sensitive networks."[132] While more information is not publicly available on this activity, it is important that the new proactive scanning task of public networks conducted in line with art. 10(2)(e) is non-intrusive, necessary, and proportionate, meaning that it abides by the human rights principles, established in the EU Charter of Fundamental Rights, and in national constitutions of Member States.

Next, the Estonian CSIRT uses a scanning device to automatically scan the state network and monitors malware in computers of the public sector administration. When an infected webpage is identified for example, the national CSIRT informs the Internet Service Provider, to further contact and inform the operator of device or webpage. Further, Estonia is developing a white hacker program through a centralised platform, which will reward white hackers that identify and report vulnerabilities. As regards vulnerability issues, RIA has an X-Road[133] platform for sharing information with the public sector in a secure way. To access the platform, a minimum standard of information security for the systems of the portal participants needs to be achieved. Healthcare centres, public institutions, hospitals, and information system agencies are all connected and the information flow is reported to take place seamlessly.

Good practice in the spotlight:
Use of Malware Information Sharing Platform (MISP)

MISP is a private non-for-profit initiative, with the aim to improve technical information sharing, indicators of compromise and malware.[134] More specifically MISP is a "software for sharing, storing and correlating indicators of compromise of targeted attacks, cybersecurity threats and financial fraud indicators."[135] MISP is broadly used by the CSIRTs community, due to its potential to share information in a timely manner and with a broad target audience of participants or a selection of those. However, not all private organisations are acquainted with the platform, and are aware how to adjust and use it in their own organisation.

[131] Christensen K and Petersen K, 'Public–private partnerships on cyber security: a practice of loyalty' (2017), Vol. 6, International Affairs, 93, 1435-1452.

[132] Centre For Cyber Security, 'CERT' (2022). <https://www.cfcs.dk/en/about-us/cert/> Accessed 27 June 2022.

[133] European Commission, 'X-Road Data Exchange Layer' (2022). <https://joinup.ec.europa.eu/collection/ict-security/solution/x-road-data-exchange-layer/about> Accessed 27 June 2022.

[134] MISP Threat Sharing, 'Home' (2022). <https://www.misp-project.org> Accessed 27 June 2022.

[135] MISP Threat Sharing, 'Information Sharing and Cooperation Enabled by GDPR' (January 2018). <https://www.misp-project.org/compliance/GDPR/> Accessed 27 June 2022.

B. Standardised processes

One of the legal tasks for CSIRTs under NIS2 is to "promote the adoption and use of common or standardised practices, classification schemes and taxonomies for incident handling procedures, cybersecurity crisis management, CVD" (art 10 (4) NIS2). Recital 28 NIS2 refers to two specific international standards on vulnerability handling and vulnerability disclosure: ISO/IEC 30111 (current version from 2019) and ISO/IEC 29147 (2018). While not mentioned in the examples offered in Recital 28, there are more existing standards on a series of CSIRT related activities. NIST for example has been developing a special publication on Recommendations for Vulnerability Disclosure Guidelines.[136]

Several MS are already using technical standards by recognised standardisation bodies such as ISO, and their own homegrown specifications (e.g. Germany and Denmark). Further, MS are often using taxonomies and classifications provided by CSIRTs communities such as FIRST, and EU bodies, such as ENISA. Standardising processes may help CSIRTs even with less complicated processes, such as standardised formats for reporting. Having a standardised format helps both with the evaluation of the incident and the sharing of information with other authorities.

Good practice in the spotlight:
Use of security standards and specifications to determine the state-of-the-art

BSI uses several ISO standards, but also homegrown non-mandatory standards, that might be useful for operators. The legal basis is the requirement of the national law, that security needs to adhere to the state-of-the-art, which is further specified by several technical standards.

The operators select the standard to conformity to together with a professional auditing company and an independent audit is conducted to the security infrastructure. The results of the audit are then submitted to BSI, which examined the audit results and decides whether the compliance with the BSI requirements has been achieved. The BSI examinations of the audit results takes place by qualified persons, who are found to be competent and independent by BSI.

Examples of homegrown 'standards' 1. IT-Grundschutz,[137] provides a method for organisations to establish and Information Security Management System 2. Sector-specific standards, "Branchenspezifische Sicherheitsstandards" (B3S). The standards are available for the energy sector, water, nutrition, IT and telecommunications sector, health, Finance and insurance, transport, and traffic.[138]

[136] NIST, Recommendations for Federal Vulnerability Disclosure Guidelines https://csrc.nist.gov/publications/detail/sp/800-216/draft (2021).

[137] BSI, 'IT-Grundschutz' (2022). <https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/IT-Grundschutz/it-grundschutz_node.html> Accessed 27 June 2022; ENISA, 'IT-Grundschutz' (2022). <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_it_grundschutz.html> Accessed 27 June 2022.

[138] BSI, 'Übersicht der Branchenspezifischen Sicherheitsstandards (B3S)' (2022). <https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/Uebersicht-der-B3S/uebersicht-der-b3s_node.html> Accessed 27 June 2022.

Another good practice from Denmark is the National Recommendations, a set of informal ‘standards’, which can be viewed as an in-depth elaboration and application of the requirements put forward in information security management system (ISMS) standards, such as the ISO/IEC 27001 series. The National Recommendations are providing also guidance on what tools constituencies are safe to use, which processes, and other relevant information.

8. Discussion and outlook for further research

The Cybersecurity landscape is ever changing and evolving. The speed with which the field is moving was obvious from the reform of the 2016 Network and Information Security Directive, which took place only a few years after the NIS1 was transposed to national legislation of the Member States. Changes in cybersecurity law are geared by the development of technologies, the growing reliance and dependence on information and security networks, and the new ways attackers exploit vulnerabilities and launch their cyber-attacks, and the effectiveness of the existing legislation. After a two-year legislative process, political agreement on NIS2 took place in May 2022.

In this fast moving, technological and regulatory landscape, cybersecurity actors in the EU countries, individually and collectively, are called to shield information security networks that are essential and important in how society functions. Within those actors, Computer Incident Response Teams (CSIRTs) are proactively and reactively offering their services to maintain and improve the level of cybersecurity of networks and information systems.

This research focused on the changes that the new EU Directive will bring to the tasks of CSIRTs and on good practices on how to (re-) organise in order to accommodate the new increased tasks and capabilities of CSIRTs. CSIRTs around the Union, have very diverse operational and organisational models. This is due to a variety of factors: the culture, organic hierarchy within a Ministry or an intelligence service, or an independent status, the countries' essential and important entities, the complexity of the organisation of cybersecurity, the past and foreseeable cyberthreats, and others. Taking this diversity into account, the study explored the different organisational models of several CSIRTs around the European Union and identified good practices that may assist CSIRTs adapting to their new tasks. Learning from other CSIRTs and adapting to own culture and mentality is a good practice in itself, in that it aims at efficiency and self-improvement of the teams. To that end, the research team conducted desk research and interviews with Member States' CSIRTs.

Key findings of the study:

- The approaches to fulfilling CSIRT tasks under NIS2 diverge strongly from one another, as do the identified good practices across Member States. However, the identified good practices are most often not mutually exclusive.
- Most of the interviewed Member States face a large growth of constituencies with the introduction of NIS2 and are currently in the process of developing strategies to accommodate new sectors and entities in their methods to perform CSIRT tasks.
- The most common problems that are faced in amending strategies revolve around scalability, ensuring access to CSIRT services for new constituents and preventing coordination risks.
- The largest differences between Member States are their centralized or decentralized approaches in the organization of (national) CSIRTs, the use of risk-based or sector-based approaches to identify and respond to threats and different forms of automation that may include portals for information sharing, notifications or tools for pro-active scanning.
- Scalability is a prominent issue as not all CSIRTs have (yet) access to the necessary resources and personnel to deal with the increase in constituencies. Expanding the

CSIRT and hiring new personnel may not be possible due to a lack of resources or a lack of candidates with the right skills and qualifications. Possible solutions for issues related to scalability may be found with automation and the standardization of protocols to use resources more efficiently, and/or by offering training programs to attract new talent.

- The use of automated tools for scanning or information sharing must happen in accordance with fundamental rights of citizens, including the right to privacy and data protection. Reliance on automated tools - in particular those for scanning - should be limited in their use and subjected to strict tests of proportionality and necessity.
- Ensuring access to CSIRT services for new constituents may arise in both centralized and decentralized approaches. Member States that rely on centralized approaches may not have the available resources, while Member States with a decentralized approach may not have set up a sectoral CSIRT for the new constituencies or may not be able to find private parties that have the capabilities to perform CSIRT tasks in these sectors yet. In order to ensure compliance with NIS2, Member States must anticipate potential bottlenecks or other obstacles in providing CSIRT tasks and develop potential solutions before the NIS2 comes into place.
- Reliance on an ecosystem of accredited and certified private actors may help CSIRTs to scale up and provide a cost-efficient way to ensure access to CSIRT services for constituents in new sectors under NIS2. However, coordination issues may arise. The national CSIRT office must set standards and requirements for certification and monitor the adherence of private CSIRTs to these standards. Periodical reviews are required as to ensure that accredited CSIRTs remain compliant over time. The national CSIRT also needs to develop protocols and methods to exercise authority over the private CSIRTs and create a complaint mechanism for constituents.
- Different approaches require the national CSIRT to fulfil different roles. The Member State must ensure that it is clear for constituents and potential public or private CSIRTs which roles the national CSIRT fulfils. The NCSC may internalize the tasks and fulfil the CSIRT tasks internally, act as a coordinator and information hub for other CSIRTs and partner organization or act as an authority over public and/or private CSIRTs. The national CSIRT may fulfil a dual role, where it acts as both a coordinator/information hub and authority. In this case, a strict separation is required between the departments that act as a partner and those that act as an authority to prevent disincentives to information sharing and cooperation by other CSIRTs or the ecosystem.

Overall, the selected Member States, including the Netherlands, are all in the process of adapting, exploring options, and translating the new legal requirements to operational, organisational, and technical measures. Several aspects would benefit from further research:

1. The meaning of the risk-based approach and concrete methodologies in prioritising CSIRT tasks in line with Art. 10(2) NIS2), [139] comparing also other EU laws, such as the General Data Protection Regulation.
2. How to fulfil the task of proactive scanning in a human-rights preserving manner (Art. 10(2)(e) NIS2).
3. Cooperation with law enforcement authorities
4. Models and degrees of automation in Incident Response and trade-offs
5. Following the concretisation of plans in different Member States, the effectiveness of a centralised or decentralised approach for the fulfilment of specific CSIRT tasks.
6. The role of CSIRTs in the upcoming regulatory framework of the Cyber Resilience Act.[140]

[139] Art. 10(2) NIS2 "When carrying out these tasks, CSIRTs may prioritise particular tasks based on a risk-based approach."

[140] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en

Annex 1: CSIRTs key tasks under NIS2

Task description	Short name	Code	Legal basis	Competence/ Requirement/ Task	Type (proactive/reactive)	New in NIS2 (new/updated/no)	Mandatory/ conditional
monitoring and analysis of cyberthreats, vulnerabilities, and incidents at national level and upon request providing support to entities regarding real time or near real time monitoring of their networks and information systems	monitoring & analysis at national level	T1	art. 10(2)(a)	CSIRT Task	proactive	updated	mandatory
providing early warnings, alerts, announcements and dissemination of information to essential and important entities as well as to competent authorities and other relevant interested parties on cyber threats, vulnerabilities and incidents, if possible in near-real-time	early warnings and dissemination of information to EE & IE & authorities& interested parties	T2	art. 10(2)(b)	CSIRT Task	reactive	updated	mandatory
responding to incidents and providing assistance to the entities concerned, where applicable	incident response	T3	art. 10(2)(C)	CSIRT Task	reactive	updated	conditional
collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity	forensic data collection and analysis	T4	art. 10(2)(d)	CSIRT Task	reactive	new	conditional
providing, upon the request of an entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact.	proactive scanning private networks upon request	T5	art. 10(2)(e)	CSIRT Task	proactive	new	conditional
CSIRTs may carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential or important entities. Such scanning shall be carried out to detect vulnerable or insecurely configured network and information systems and inform the entities concerned. Such scanning shall not have any negative impact on the functioning of their services	proactive scanning public networks	T6	art. 10(2)(e)	CSIRT Task	proactive	new	conditional
participating in the CSIRTs network and providing mutual assistance according to their capacities and competencies to other members of the network upon their request.	CSIRTs network members support	T7	art. 10(2)(f)	CSIRT Task	proactive	new	mandatory
where applicable, acting as a coordinator for the purpose of the coordinated vulnerability disclosure process pursuant to Article 6 (1) that shall include in particular facilitating the interaction between the reporting entities, the potential vulnerability owner and the manufacturer or provider of ICT products or ICT services in cases	CVD coordinator and management subtasks	T8	art. 10(2)(fa) art. 6(1)	CSIRT Task	reactive	new	conditional

where this is necessary, identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure time lines and managing vulnerabilities that affect multiple organisations (multi-party coordinated vulnerability disclosure).							
contributing to the deployment of secure information sharing tools pursuant to Article 9(3).	secure information sharing tools	T9	art. 10(2)(fb)	CSIRT Task	proactive	new	mandatory
CSIRTs shall establish cooperation relationships with relevant actors in the private sector, with a view to better achieving the objectives of the Directive	cooperation with private actors	T10	art. 10 (3)	CSIRT Task	proactive	updated	mandatory
Where they are separate, the competent authorities referred to in Article 8, the single point of contact and the CSIRT(s) of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive	national cooperation	T11	art. 11	CSIRT Task	proactive	no	mandatory
CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies for incident handling procedures, cybersecurity crisis management, CVD.	promotion of standardised practices	T12	art 10 (4)	CSIRT Task	proactive	updated	mandatory
the CSIRT may receive an art. 20 report for incidents having significant impact. the CSIRT may request an intermediate report on relevant status updates by the essential and important entities in line with art. 20(1)	intermediate report request	P1	art. 20 (1) (c)	CSIRT power	reactive	new	conditional
the CSIRT shall provide without undue delay [..] a response to a notifying entity, including initial feedback and upon request, guidance or other operational advice. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected of criminal nature, the CSIRT shall provide guidance on reporting the incident to the LEAs.	response to incidents with significant impact	T13	art. 20 (5)	CSIRT Task	reactive	new	mandatory

Annex 2: Interviewed organisations

The Netherlands	NCSC -NL
	NCTV
Germany	CERT-Bund and BSI
Estonia	CERT-EE at Estonian Information System Authority
Denmark	CSIRT at RIA (Systems information Authority)
Austria	CERT.at
France	CERT-FR at ANSSI

Annex 3: Interview Questions for National CSIRTs

1. **General Questions about CSIRT in the Member State**

- Could you state your name, title, and affiliation?
- Who exercises the CSIRT tasks in your country?
- Are the tasks under the Network and information security directive - EU 2016/1148 divided among more than one entity? Which ones?
- To which ministry this organisation belongs?
- Is the CSIRT part of the national cybersecurity authority?
- How is the CSIRT organised in your country? Which units?
- Approximately how many constituencies belong now in the competence of the CSIRT in your country? Does this correspond to the current NIS Directive categorisation?
- The upcoming reform of the NIS Directive is expected to change the sectors but also the fact that MS do not have to identify the entities anymore (art. 5 NIS). Is there a similar large increase expected for the CSIRT in your country?
- Which areas will be impacted in terms of organisation/processes/staffing/tools from the reform?
- General question: Which (concrete) steps does your country take to deal with this increase?
- Will there be changes in terms of internal organisation of the CSIRT?

2. **Incident response questions**

- How can an entity report an incident?
- Which team in your CSRIT is responsible for incident reception and response? Is there a first response team/centre that assigns the incidents to another team? On the basis of which criteria?
- How can an entity report an incident?
- Which team in your CSRIT is responsible for incident reception and response? Is there a first response team/centre that assigns the incidents to other team? On the basis of which criteria?
- Is there a template form available with the required information?
- How are entities informed whom they need to inform for their incidents?
- Does every incident report automatically open a new case/ticket in the system? What program do you use? How are incidents categorised, organised, prioritised?
- Urgency, amount of possible affected entities/persons, severity of the threat?
- Could you describe the process from the moment a report is received until analysis, handling, possible follow-up?
- Do you follow any technical standards for incident response?
- Are some processes (e.g. compiling a report) automated?
- How do you ensure accuracy of the information – (facts versus speculation)?
- With which technical means do you share information with the other departments of the CSIRT or other affected entities?
- How do you select what information to share and with whom? Is there a policy/process for this?
- What is the timeframe for:
    - reacting to a reported incident?
    - Sharing information with other entities in the sector? Other public entities? Authorities in other countries?
- How are those processes and timeframes decided?
- What skills do the national CSIRT experts that handle incident response have? Do you have in-house only experts or do you collaborate with other ministries/CERT (computer emergency response teams)/ private consultants under confidentiality agreements?

- In terms of incident response and handling, which do you consider good practices in your CSIRT team that could be an example for other national CSIRTs?

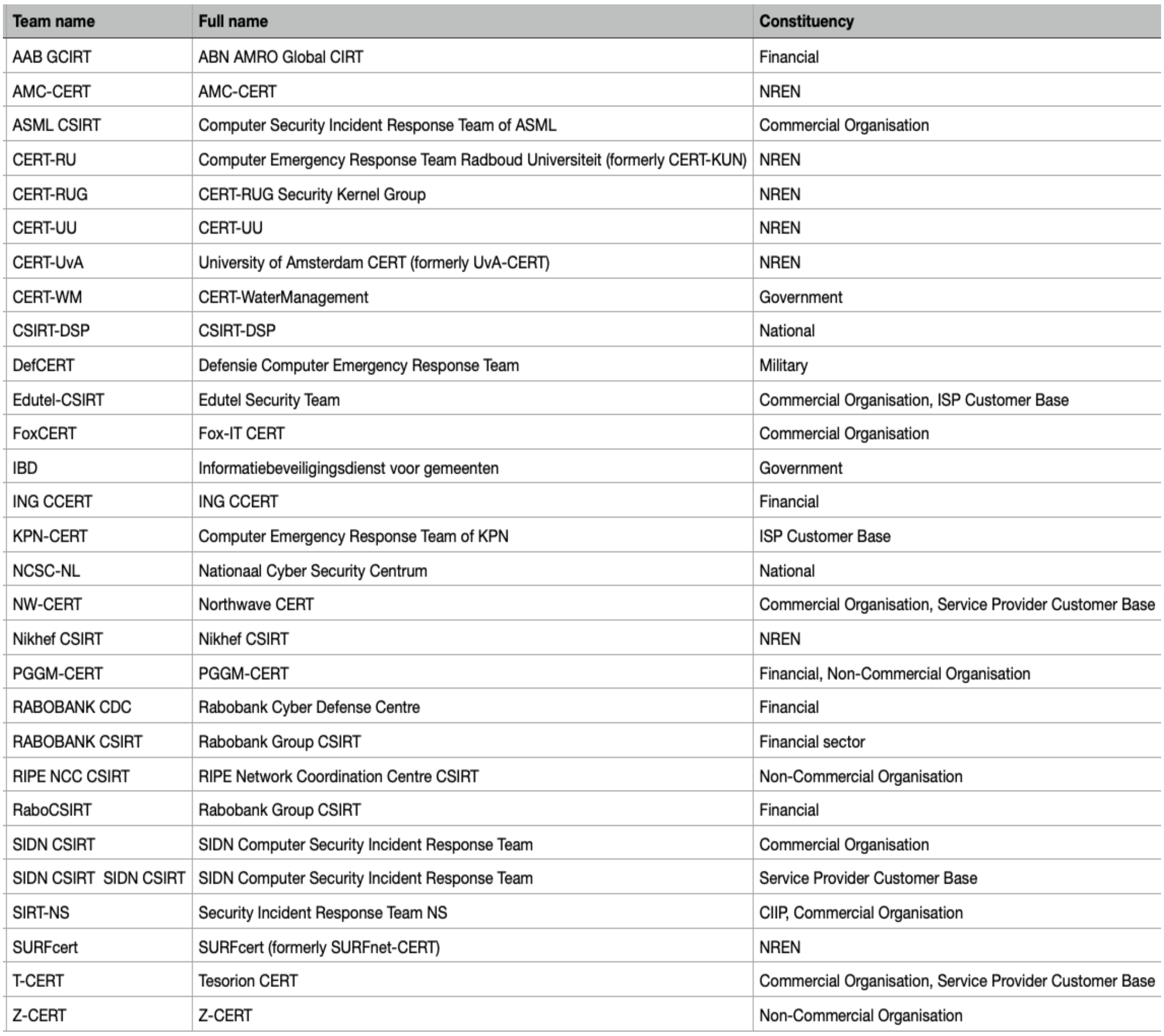
3. International and national cooperation

- Under the NISD2, CSIRTs are expected to contribute to the "development of confidence and trust between the MS and to promote swift and effective operational cooperation": How do you plan to respond to and organise this role?
- NISD2 foresees the division between essential and important services: where do you draw the line in sharing information, given that some information obtained by essential services might be useful for providers of important services?
- How is vulnerability disclosure taking place now?
- Do you follow any standards (e.g.NIST: https://www.iso.org/standard/72311.html or ISO/IEC 29147: 2018)?
- How (processes, tools – automation) the Single Point of Contact will forward incident notification?
- NISD2 (Council) foresees cooperation arrangements among MS, and that MS must set up processes to address on-site inspections and sharing information on cyberinvestigations.
- Currently in NL- NCSC, there are three collaboration manners: 1. Sectoral cooperation - Information Sharing and Analysis Centres (ISACs), 2. Regional cooperation 3. Cooperation within supply chain.
- Does something similar exist or is envisaged to be developed in view of NISD2? What other ways to bring together different stakeholders exist in your organisation (or plan to develop)?
- What is a good practice to deal with interoperability issues in sharing information?
- In terms of international and national cooperation, which do you consider good practices in your CSIRT team that could be an example for other national CSIRTs?

4. Tools

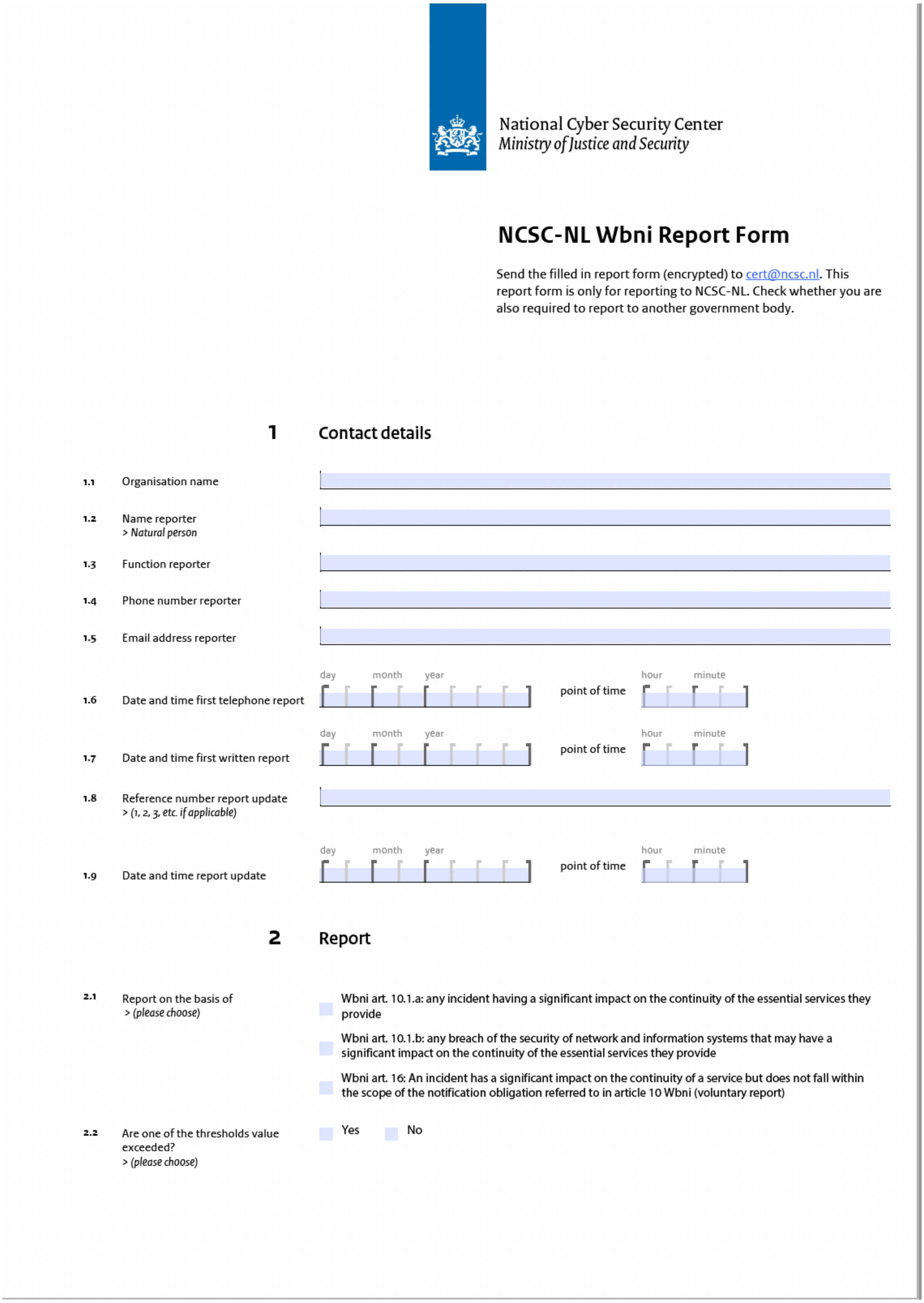
- In terms of technical research, monitoring and tools, which do you consider good practices in your CSIRT team that could be an example for other national CSIRTs?

Annex 4: CSIRT teams in The Netherlands (source ENISA)



Team name	Full name	Constituency
AAB GCIRT	ABN AMRO Global CIRT	Financial
AMC-CERT	AMC-CERT	NREN
ASML CSIRT	Computer Security Incident Response Team of ASML	Commercial Organisation
CERT-RU	Computer Emergency Response Team Radboud Universiteit (formerly CERT-KUN)	NREN
CERT-RUG	CERT-RUG Security Kernel Group	NREN
CERT-UU	CERT-UU	NREN
CERT-UvA	University of Amsterdam CERT (formerly UvA-CERT)	NREN
CERT-WM	CERT-WaterManagement	Government
CSIRT-DSP	CSIRT-DSP	National
DefCERT	Defensie Computer Emergency Response Team	Military
Edutel-CSIRT	Edutel Security Team	Commercial Organisation, ISP Customer Base
FoxCERT	Fox-IT CERT	Commercial Organisation
IBD	Informatiebeveiligingsdienst voor gemeenten	Government
ING CCERT	ING CCERT	Financial
KPN-CERT	Computer Emergency Response Team of KPN	ISP Customer Base
NCSC-NL	Nationaal Cyber Security Centrum	National
NW-CERT	Northwave CERT	Commercial Organisation, Service Provider Customer Base
Nikhef CSIRT	Nikhef CSIRT	NREN
PGGM-CERT	PGGM-CERT	Financial, Non-Commercial Organisation
RABOBANK CDC	Rabobank Cyber Defense Centre	Financial
RABOBANK CSIRT	Rabobank Group CSIRT	Financial sector
RIPE NCC CSIRT	RIPE Network Coordination Centre CSIRT	Non-Commercial Organisation
RaboCSIRT	Rabobank Group CSIRT	Financial
SIDN CSIRT	SIDN Computer Security Incident Response Team	Commercial Organisation
SIDN CSIRT SIDN CSIRT	SIDN Computer Security Incident Response Team	Service Provider Customer Base
SIRT-NS	Security Incident Response Team NS	CIIP, Commercial Organisation
SURFcert	SURFcert (formerly SURFnet-CERT)	NREN
T-CERT	Tesorion CERT	Commercial Organisation, Service Provider Customer Base
Z-CERT	Z-CERT	Non-Commercial Organisation

Annex 5: Incident Reporting form under the national Dutch law implementing NIS (wbni)



National Cyber Security Center
Ministry of Justice and Security

NCSC-NL Wbni Report Form

Send the filled in report form (encrypted) to cert@ncsc.nl. This report form is only for reporting to NCSC-NL. Check whether you are also required to report to another government body.

1 Contact details

1.1 Organisation name

1.2 Name reporter
> *Natural person*

1.3 Function reporter

1.4 Phone number reporter

1.5 Email address reporter

1.6 Date and time first telephone report — day month year — point of time — hour minute

1.7 Date and time first written report — day month year — point of time — hour minute

1.8 Reference number report update
> *(1, 2, 3, etc. if applicable)*

1.9 Date and time report update — day month year — point of time — hour minute

2 Report

2.1 Report on the basis of
> *(please choose)*

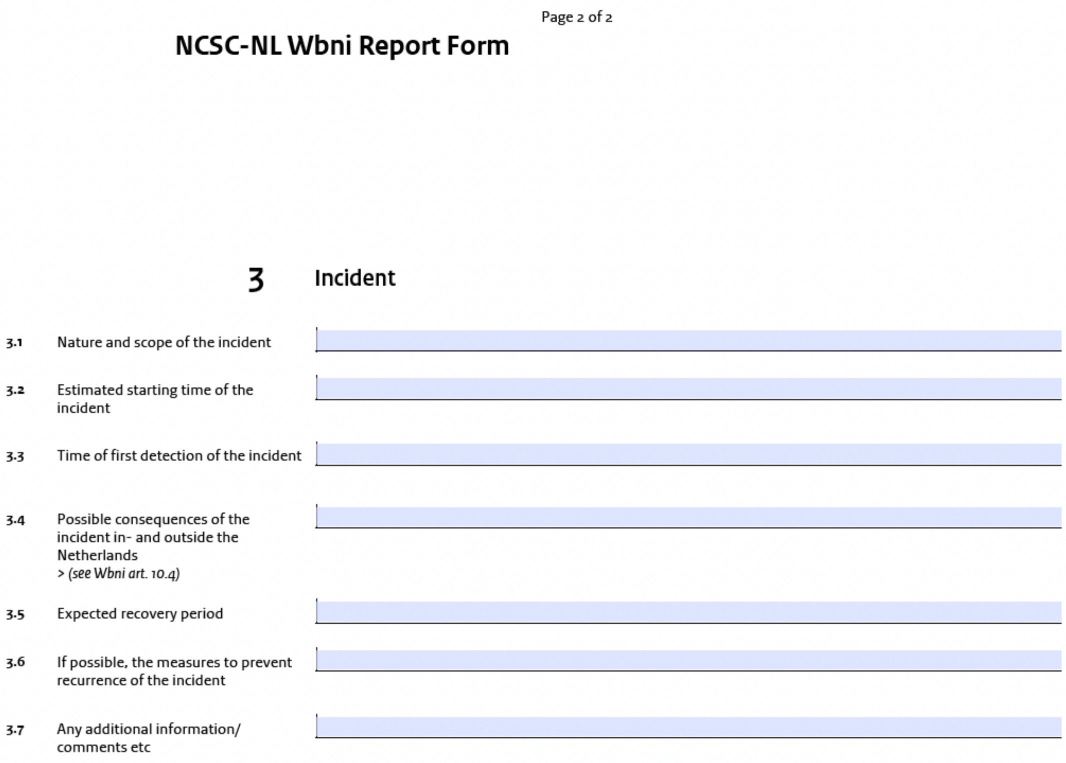
□ Wbni art. 10.1.a: any incident having a significant impact on the continuity of the essential services they provide

□ Wbni art. 10.1.b: any breach of the security of network and information systems that may have a significant impact on the continuity of the essential services they provide

□ Wbni art. 16: An incident has a significant impact on the continuity of a service but does not fall within the scope of the notification obligation referred to in article 10 Wbni (voluntary report)

2.2 Are one of the thresholds value exceeded?
> *(please choose)*

□ Yes □ No



Page 2 of 2

NCSC-NL Wbni Report Form

3 Incident

3.1 Nature and scope of the incident

3.2 Estimated starting time of the incident

3.3 Time of first detection of the incident

3.4 Possible consequences of the incident in- and outside the Netherlands
> (see Wbni art. 10.4)

3.5 Expected recovery period

3.6 If possible, the measures to prevent recurrence of the incident

3.7 Any additional information/ comments etc

Bibliography

Alberts, Chris; Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin and Zajicek, Mark. "Defining Incident Management Processes for CSIRTs: A Work in Progress" (2004), Technical Report.

ANSSI. "Annual Review" (2021)

ANSSI. "The ANSSI Security Visa by the French National Cybersecurity Agency" (2022).

Besluit aanwijzing toezichthouders Wet beveiliging netwerk- en informatiesystemen [...] energie, digitale infrastructuur en voor digitale diensten 2018.

Besluit van de Minister van Justitie en Veiligheid van 28 november 2017, kenmerk DP&O/17/2150354, houdende vaststelling van de organisatie van het Ministerie van Justitie en Veiligheid (Organisatiebesluit Ministerie van Justitie en Veiligheid).

Bekkers L. et al, Verkenning best Practices cybersecurity Informatiedeling (2020)

BSI. "Allianz für Cyber-Sicherheit" (2022).

BSI. "RFC 2350" (2017).

BSI. "Übersicht der Branchenspezifischen Sicherheitsstandards (B3S)" (2022).

Brownlee, N. and Guttman, E. "Expectations for Computer Security Incident Response" (1998).

Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) (2018).

Bundeskanzelaramt & Bundesministerium Inneres. "Kontaktstellen von Betreibern wesentlicher Dienste" (2019), NIS Fact Sheet 1/2019 – Version 2.

Centre for Cyber Security. "CERT" (2022).

CERT.at. "RFC 2350" (2021).

CERT-FR. "CERT-FR description – RFC 2350" (2018).

Christensen K and Petersen K, 'Public–private partnerships on cyber security: a practice of loyalty' (2017), Vol. 6, International Affairs, 93, 1435-1452.

Cichonski, Paul; Millar, Tom; Grance, Tim and Scarfone, Karen. "Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology" (NIST 2012), Special Publication 800-61, Revision 2.

Council of the European Union, Directive (EU) 2022/...Of The European Parliament And Of The Council, on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), repealing Directive (EU) 2016/1148 (Dossier interinstitutionnel: 2020/0359(COD)), 17 June 2022 (NIS2 Political Agreement text) https://data.consilium.europa.eu/doc/document/ST-10193-2022-INIT/x/pdf.

CSIRTs Network. "CSIRTs Network" (2022).

Cyberwise. "Infosheet Dutch Cybersecurity Agenda" (2020).

Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

Deloitte. "Cyber security in the Netherlands: a responsibility we share. Dutch cyber security survey" (2021).

DFN CERT. "CSIRT Description for DFN-CERT" (2022).

De Nederlandse Grondwet. "Herziening richtlijn netwerk- en informatiebeveiliging (NIB-richtlijn)" (2021).

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.

Dulaunoy, Alexandre. “CTO and Automation. Supporting CSIRT capabilities and reduce manual operations” (2020), presentation CTI-EU event.

EGC group. “European Government CERTs (EGC) group” (2022)

ENISA. “A step-by-step approach on how to setup a CSIRT. Including examples and a checklist in form of a project plan” (2006), Deliverable WP2006/5.1, CERT-D1/D2,

ENISA. “CSIRT Maturity Assessment Framework – Updated and improved” (2022)

ENISA. “Good practice guide for CERTs in the area of Industrial Control Systems. Computer Emergency Response Capabilities considerations for ICS” (2013),

ENISA. “How to setup up CSIRT and SOC. Good Practice Guide” (2020),

ENISA. “IT-Grundschutz“ (2022)

ENISA. “Reference for an Incident Response Taxonomy. Task Force Status and Way Forward” (2018)

ENISA. “SIM3v1 self-assessment tool” (2022)

European Commission. “Commission staff working document – Impact Assessment Report – Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148” (2020), SWD, 345 final.

European Commission. “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.

European Commission. “Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union”, COM/2013/048 final - 2013/0027 (COD).

European Commission. “X-Road Data Exchange Layer” (2022), https://joinup.ec.europa.eu/collection/ict-security/solution/x-road-data-exchange-layer/about.

Europol. “European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021. A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime” (2019).

FIRST. “Bylaws of FIRST.Org, Inc.” (2022).

FIRST. “Computer Security Incident Response Team (CSIRT) Services Framework” (2019),

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) (2009).

Global Forum on Cyber Expertise. “GFCE Global Good Practices. National Computer Security Incident Response Teams (CSIRTs)” (2017), Global Conference on Cyber Expertise 2017.

Global Forum on Cyber Expertise. “Launch of the Global Forum on Cyber Expertise. 16 April 2015. The Hague Declaration on the GFCE” 2015, Global Conference on Cyber Expertise 2015.

GovCERT Austria. “GovCERT Austria RFC 2350” (2021).

ISO, ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management (2016).

Justice and Security Inspectorate. “Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021” (2008), 8.

Kamara, Irene; Leenes, Ronald; Stuurman, Kees and Van den Boom, Jasper. “The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act” (Tilburg University, 2020).

Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin and Zaijcek, Mark. "Organizational Models for Computer Security Incident Response Teams (CSIRTs)" (CarnegieMellon 2003), Handbook.

Killcrece, Georgia. "Steps for Creating National CSIRTs" (2004).

Lacity M and L Willcocks, *Robotic process and cognitive automation: the next phase* (SB Publishing 2018).

Luijf, Eric and Kernkamp, Allard. "Sharing Cyber Security Information. Good Practice Stemming from the Dutch Public-Private-Participation Approach" (March 2015), Global Conference on Cyber Space 2015.

Ministry of Justice and Security. "Beleidsreactie CSBN 2021 en voortgangsrapportage NCSA" (2021), Kamerstukken 26 643.

Ministry of Justice & Security. "Brief van de Minister van Justitie & Veiligheid aan de Voorzitter van de Tweede Kamer der Staten-Generaal omtrent de verkenning van wettelijke bevoegdheden digitale weerbaarheid en beleidsreacties" (2021), Kamerstukken 26 643.

MISP Threat Sharing. "Information Sharing and Cooperation Enabled by GDPR" (2018)

National Cyber Security Centre. "CNI Hub" (2022)

National Cyber Security Centre. "Certified Cyber professional (CCP) assured service" (2018).

NCSC. "Aansluiting op het Landelijk Dekkend Stelsel (LDS)" (2022).

NCSC. "Coordinated Vulnerability Disclosure: the Guideline" (2018).

NCSC. "CVD-report form" (2022).

NCSC. "Het Traffic Light Protocol" (2022).

NCSC. "International cooperation" (2022).

NCSC. "Start zelf een samenwerking" (2022).

NCTV. "Nationaal Crisisplan Digitaal" (2020).

Onwubiko C, 'CyberOps: Situational Awareness in Cybersecurity Operations' (2022), Vol. 5, International Journal on Cyber Situational Awareness.

Organization of American States. "Best Practices for Establishing a National CSIRT" (2016).

Onlinesicherheit.at. "Austrian Trust Circle (ATC)" (2022).

Pitt, L. "Security Automation Challenges to Adoption: Overcoming Preliminary Obstacles" (*Securityweek*, 10 July 2020).

Republic Of Estonia Information System Authority. "RFC 2350 Description for CERT-EE" (2020).

Serrat, O. *Knowledge Solutions* (Springer 2017), 843-846.

Skierka, Isabel; Morgus, Robert; Hohmann, Mirko and Maurer, Tim. "CSIRT Basics for Policy-Makers" (2015), Working Paper.

Threat Intelligence. "Automated Incident Response: What It Is, Tools and Use Cases" (*Threat Intelligence*, 23 August 2021.

UP KRITIS. UP KRITIS. "Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen" (2014).

Van den Berghe, Michel. "Cyber Campus. Uniting and Expanding the Cybersecurity Ecosystem"(2020).

Van der Heide, M. "Establishing a CSIRT" (2017), version 1.2.

Van der Meulen N, 'Stepping out of the Shadow: Computer Security Incident Response Teams in the Cybersecurity Ecosystem' (2021), The Oxford Handbook of Cyber Security, 297.

Wet van 17 oktober 2018, houdende regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen).

WODC. “Evaluatie van de opbouw en meetbaarheid van de Nederlandse Cybersecurity Agenda” (2021), Final Report.

Wiik, Johannes; Gonzales, Jose and Kossakowski, Klaus-Peter. “Effectiveness of Proactive CSIRT Services“ (2006).

Wiik, Johannes; Gonzales, Jose; Davidsen, Pal and Kossakowski, Klaus-Peter. “Persistent instabilities in the high-priority incident workload of CSIRTs” (2009), 27th International Conference of the System Dynamics Society.

Weiss M and Biermann F, ’Cyberspace and the protection of critical national infrastructure’ (2021), Journal of Economic Policy Reform.