EUROPEAN UNION AGENCY
FOR CYBERSECURITY

A GOVERNANCE FRAMEWORK FOR NATIONAL CYBERSECURITY STRATEGIES

February 2023

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For contacting the authors please use team@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Anna Sarri, Gema Fernández Bascuñana (ENISA)
Ann-Kristin Gross, Federico Chiarelli, Marina Preasca (Wavestone)

ACKNOWLEDGEMENTS

ENISA would like to thank and acknowledge all the expert that took part and provided valuable input for this report and especially the following, in alphabetical order:

Andrés Jesus Ruiz Vazquez (Spain);
Center for Cyber Security (Denmark), Chief Advisor;
Centre for Cybersecurity (Belgium);
Croatian National Security Authority, Senior Advisor, Vinko Kuculo;
Cyber Security Coordination and Policy Department (the Netherlands), Gijs Peeters;
Cyber Security Coordination and Policy Department (the Netherlands), Pieter van den Berg;
Department for Secure Communication, Senior Advisor and Sweden's Liaison Officer to ENISA (Sweden), Peter Wallström;
Department of Environment, Climate & Communications, Staff Engineer, Cyber Security & Internet Policy Division (Ireland), James Caffrey;
Digital Security Authority of Cyprus, Technical Officer, Costas Efthymiou;
Digital Security Authority of Cyprus, Technical Officer, Giorgos Loninos;
Federal Chancellery, Department I/8 – Cyber Security, GovCERT, NIS-Office and ZAS (Austria), Deputy Head, Christian Zec;
Federal Ministry of the Interior (Germany), Sascha-Alexander Lettgen;
International Server Security Authority (Greece), Head of Competent Department for Cyber Security Strategic Planning, Emmanouil Patsourakis;
International Server Security Authority (Greece), Head of the Directorate for Cyber Security, Ioannis Alexakis;
Malta Information Technology Agency, Katia Bonello;
Malta Information Technology Agency, Martin Camilleri;
Ministry of Home Affairs, Security, Reforms and Equality (Malta);
Ministry of Economic Affairs and Communication, Department of National Cyber Security (Estonia), Kristjan Kaskman;
Ministry of Economic Affairs and Communication, Department of National Cyber Security (Estonia), Martin Sepp;
Ministry of National Defence of Lithuania;
National Cybersecurity Agency (Italy);
National Cyber and Information Security Agency, National Strategy and Policy Unit (Czech Republic), Tomáš Kellner;
National Cyber Security Centre (Finland), Olli Lehtilä;
National Security Authority (Slovakia).

ENISA would also like to thank for their valuable contribution to this study, all the experts that provided input, but prefer to stay anonymous.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.
This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPRYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2023
Reproduction is authorised provided the source is acknowledged.

Copyright for the image on the cover and on cover page: © Shutterstock
For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

ISBN: 978-92-9204-589-0

DOI: 10.2824/211856

Catalogue number: TP-04-22-152-EN-N

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SCOPE, OBJECTIVES & AIM

The EU Cybersecurity Act states that ENISA shall support the Member States in developing national strategies on the security of network and information systems, promote the correct deployment of those strategies and set up a governance framework that ensures the sustainability of national strategies (National Cybersecurity Strategy - NCSS). As part of this mandate, ENISA launched this study to perform a systematic review of the governance models relevant to the deployment of an NCSS to identify and select the most relevant instances, lessons learned, and good practices from the Member States.

This study aims to collect insights on the definition of processes, roles and responsibilities, the subsequent deployment of monitoring measures and what are the main challenges and good practices that the European countries put in place to ensure an effective governance framework for the implementation of current and future NCSSs of the EU Member States.

DEFINITIONS

CYBERSECURITY ACT (CSA)

The CSA establishes a cybersecurity certification framework and introduces rules for EU-wide certification of ICT products, processes and services. Additionally, it grants ENISA a permanent mandate and increased responsibilities and resources to support cybersecurity across the Union.

GOVERNANCE

Governance describes a complex system, defining roles, responsibilities, processes and relationships. Governance includes stakeholders from and covers the private sector, the public administration as well as the civil society and spans over different topics such as economic, social and political priorities.

CYBER GOVERNANCE

“Operation of decision-making processes” which increase and ensure “participation, transparency, and accountability in taking measures related to cyberspace together with the mechanism of international agreements, strategies, laws, measures, regulations, and standards that interlock in the best way” (Efe & Bensghir, 2019).

GOVERNANCE MODEL

A governance model provides a framework to systemise and organise stakeholders, actions, processes, and relationships to reach defined objectives of a policy, strategy or political system. This study assesses governance models based on their political, strategic, operational and technical elements to reach the objectives of the NCSS.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

METHODOLOGICAL APPROACH

1

Desk Research: The desk research has been focused on good practices adopted in the EU Member States, while insights collected from around the world complement the analysis.

2

Collection of experts and stakeholders' points of view: In this context, 19 stakeholders from 18 EU Member States have been interviewed. The national stakeholders have all been part of the national authority or government body in charge of the cybersecurity strategy.

3

Analysis of data: The data collected through desk research and interviews was analysed to identify good practices in the design of a governance framework.

4

Definition of good practices for governance: Thereafter, good practices and trends in setting up governance models have been defined and validated by national experts, before publication.

INTERVIEWED MEMBER STATES

18 Member States interviewed

- Austria
- Belgium
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- Germany
- Greece
- Ireland
- Italy
- Lithuania
- Malta
- Netherlands
- Slovakia
- Spain
- Sweden

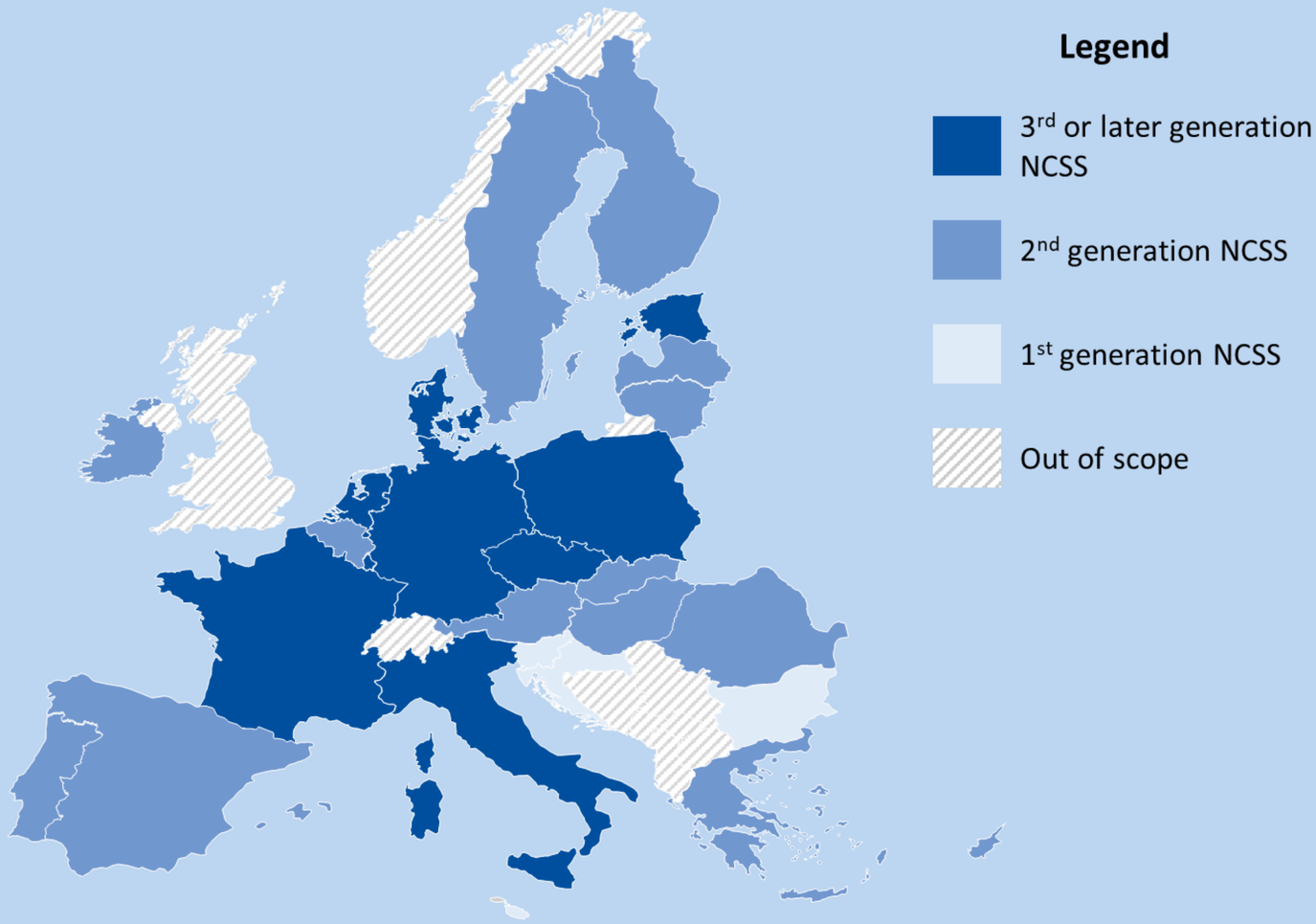
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

THE NCSSs in the EU

NCSS generation in the EU

Out of the 27 Member States:

- 9 Member States have 3rd or later generation NCSS;
- 14 Member States have a 2nd generation NCSS;
- 4 Member States are at their first NCSS.



Every EU Member State is obliged, following the NIS Directive, to develop and implement a National Cybersecurity Strategy (NCSS) to ensure fostering security of network and information systems across the Union. Each NCSS aims to set out a plan of actions to improve the security and resilience of national infrastructure systems and services. It aims to provide a high-level top-down approach to cybersecurity and to establish a range of national objectives and priorities.

However, the fast and ever-evolving cyberspace calls for constantly developing and adopting the NCSS and hence consistent monitoring and evaluation of the NCSS is necessary.
Additionally, establishing a functioning and effective governance model for the implementation of the current and future NCSSs is essential to foster cybersecurity across the Union and to reach the national strategies' as well as the institutions' objectives in this relation.

The creation of a central body in charge of the successful deployment of the NCSS is uniquely affected by the type of government or its self-governance.

Some of the factors that play a role in the definition of the mandate of such a body are related to the dimension of the country, stage of maturity and the country's self-governance.

100%

of the interviewed stakeholders have in place a central cybersecurity body.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

DEVELOPING AN EFFECTIVE GOVERNANCE MODEL FOR NCSSs

STRATEGIC GOVERNANCE

Coordinates the processes of drafting the strategy and building the governance model from the outset.

Ensures cooperation for identifying and mitigating risks.

OPERATIONAL GOVERNANCE

Ensures translation of NCSSs into actions to improve cybersecurity across the society.

Aims to increase cybersecurity across all levels and sectors of a nation's society, economy, and government.

TECHNICAL GOVERNANCE

Encompasses the definition and use of standards and specifications.

Ensures inclusion of tools, technology, and certification schemes accompanying the implementation of the strategy.

POLITICAL GOVERNANCE

Provides general and legal framework and establishes processes, roles and responsibilities.

Ensures accountability, transparency and acceptance of the NCSSs, its policies and all related processes.

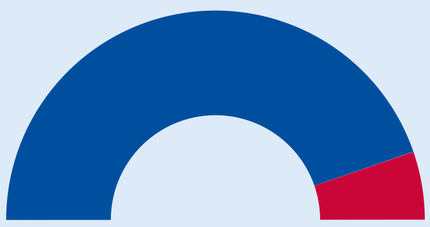
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Elements of Political Governance

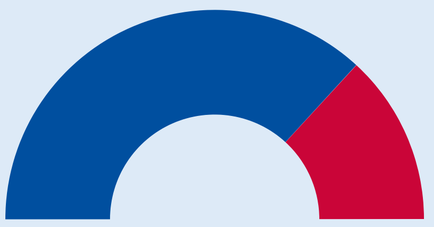
Overview of the implementation status across the interviewed EU Member States

POLITICAL PROCESSES

Focus on cooperative and collaborative approaches at international, inter-sectoral and regional levels

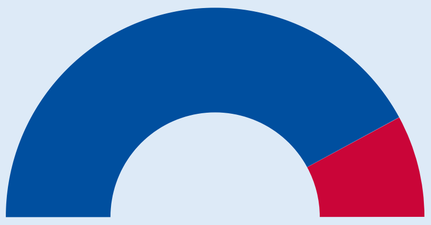


Focus on participatory approaches, including various stakeholder groups

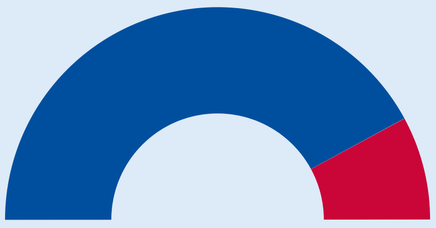


Collaboration with PPPs

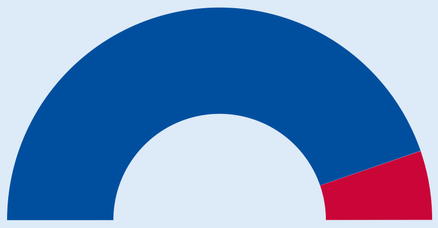
ROLES AND RESPONSIBILITIES



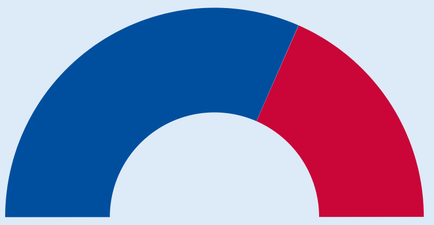
Creation of specialised government authorities, bodies and agencies to ensure governance of cybersecurity



Clear definition of responsibilities, definition of roles and tasks in case of incidents

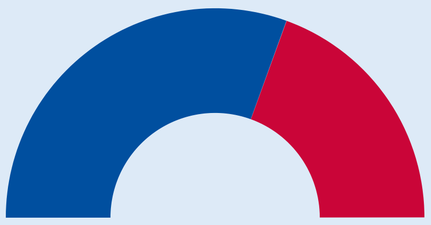


Creation of roles and allocation of responsibilities in relation to international cooperation on cybersecurity

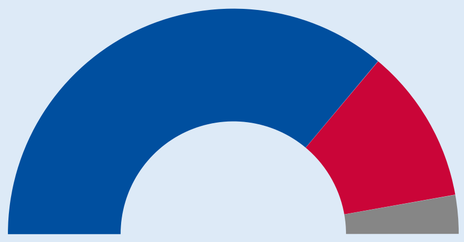


Creation of PPPs

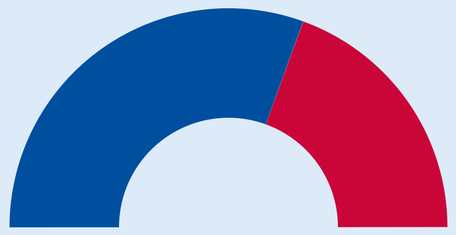
LEGAL MEASURES



Establishment of a legal governance/legal framework linked to specific legal measures



International cooperation in relation to legal measures



Emphasis on human rights in legal measures/legal framework

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Good Practices for Political Governance

Political processes

- Provide political support in the development and implementation of NCSS and governance models.
- Ensure adequate coordination and cooperation among the relevant players.
- Build trust between the different stakeholders.
- Follow participatory approaches by putting in place platforms of exchange
- Ensure support from the highest political level in the creation of Public-Private Partnerships.

Involve all stakeholders in the process

- Involve all stakeholders in the process of developing an NCSS and a governance model (choose the right level of representation for the different stakeholders)
- Set up a collaborative platform to monitor the progress of the action plan.
- Create a monitoring plan for entities in the domain of cybersecurity.
- Define a concrete accompanying Action Plan to set out measures for implementing the objectives of the strategy.

Roles and responsibilities

- Mandate a single body to ensure the coordination and the implementation of the overall strategy.
- Precisely define roles and responsibilities of the different stakeholders involved in the governance model in one document.
- Create PPPs.

Legal measures

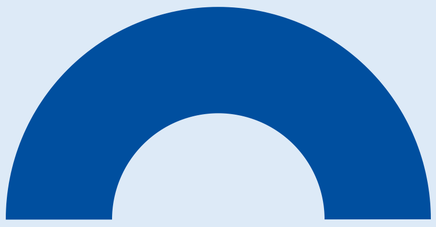
- Ensure that the governance framework is supported by and defined in accordance with the legal framework.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

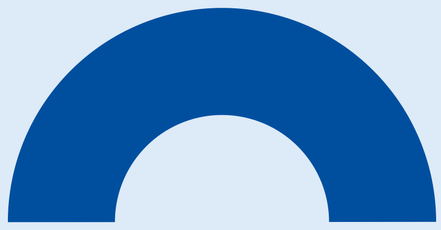
Elements of Strategic Governance

Overview of the implementation status across the interviewed EU Member States

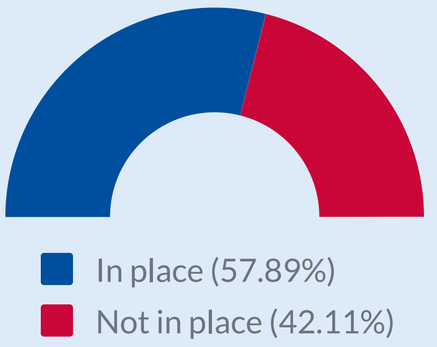
THE NCSS AND ITS IMPLEMENTATION



Pre-defining a governance model for the implementation of the NCSS in parallel to drafting the NCSS

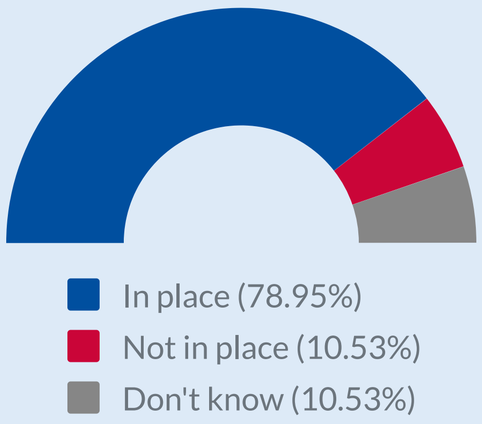


Institutional support foreseen to implement the NCSS

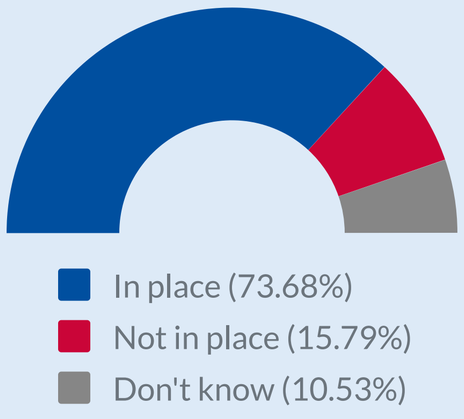


Risk identification and mitigation supported by created agencies

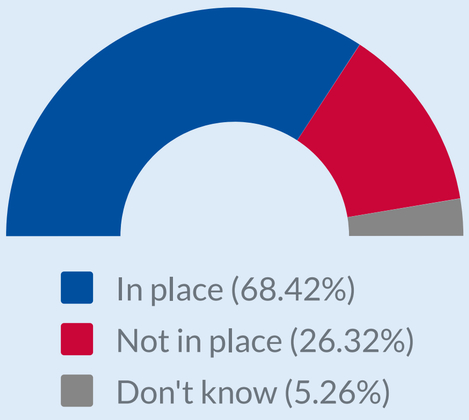
STRATEGIC ASPECTS OF RISK IDENTIFICATION AND MITIGATION



Planning of allocation of budget and resources and integration of cybersecurity into the use of these



Coherent approach for risk identification & mitigation across government entities and other critical infrastructure operators



Mechanisms to ensure accountability, transparency, and human rights during risk identification & mitigation

Good Practices for Strategic Governance

In Relation to the NCSS and its implementation

- Develop the budget from bottom to top.
- Include a paragraph on financials in NCSS.
- Definition of accountability and transparency rules.
- Include legislation ensuring human rights in the NCSS.

Strategic aspects of risk identification and mitigation

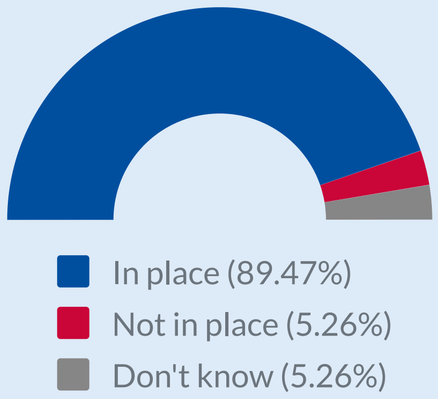
- Follow a common methodology for risk identification.
- Thorough risk identification across different levels.
- Early on identification of risks and implementation of risk assessment mechanisms.
- Follow a common framework in case of incidents.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

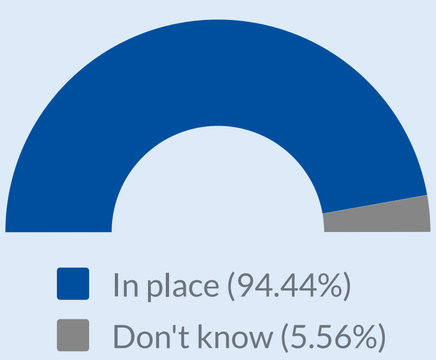
Elements of Operational Governance

Overview of the implementation status across the interviewed EU Member States

AWARENESS RAISING

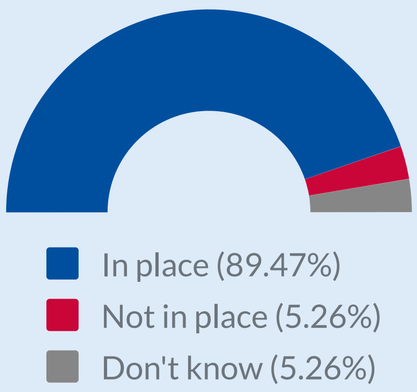


Awareness raising, knowledge and capacity building within the complete workforce/population



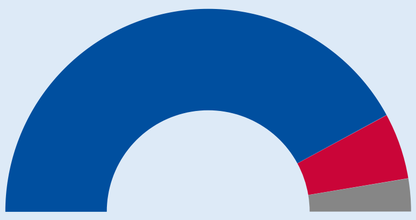
Awareness raising, knowledge and capacity building within the cybersecurity relevant workforce

INCIDENT RESPONSE



Incident response mechanisms and support of CSIRTs/CERTs

INFORMATION SHARING



Information sharing processes during the incident response (formal and informal)

Good Practices for Operational Governance

Awareness Raising

Tailored awareness raising and training campaigns.

Incident Response

Formalise a coordinated approach between CSIRTs.

Information Sharing

Centralise information sharing.

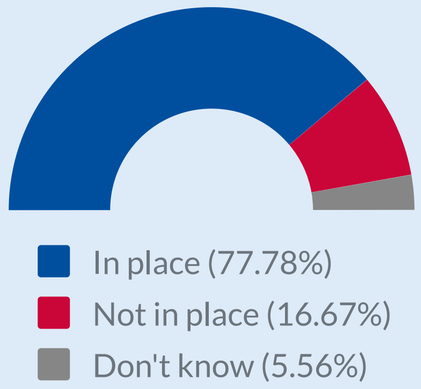
Taxonomy of best practices to ensure coherent processes of information sharing.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Elements of Technical Governance

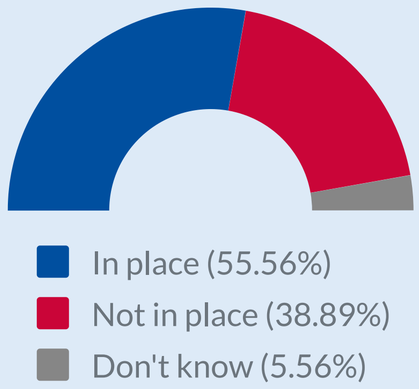
Overview of the implementation status across the interviewed EU Member States

INTERNATIONAL STANDARDS & TECHNICAL GUIDELINES



Technical governance for cybersecurity based on international standards and technical guidelines

USE OF TOOLS, TECHNOLOGY AND CERTIFICATION SCHEMES



Implemented/defined use of tools and technology

Good Practices for Technical Governance

International Standards and Technical Guidelines

Develop in the NCSS and its governance model a section focused on the international standards and technical guidelines. When developing this section, specify which technical standards should be used, and define clear roles and responsibilities.

Use of Tools, Technology, and Certification Schemes

Have in place a body that supervises the compliance of regulated entities with the European and international requirements.

Use certification schemes for ICT products, ICT services and ICT processes, especially for all the services or activities provided by essential entities. The competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning part or all the services provided by an essential entity.

Put in place in the NCSS action plan a group of tasks focused on using tools and technologies in respect to human rights, particularly to GDPR.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TP-04-22-152-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-589-0
DOI: 10.2824/211856