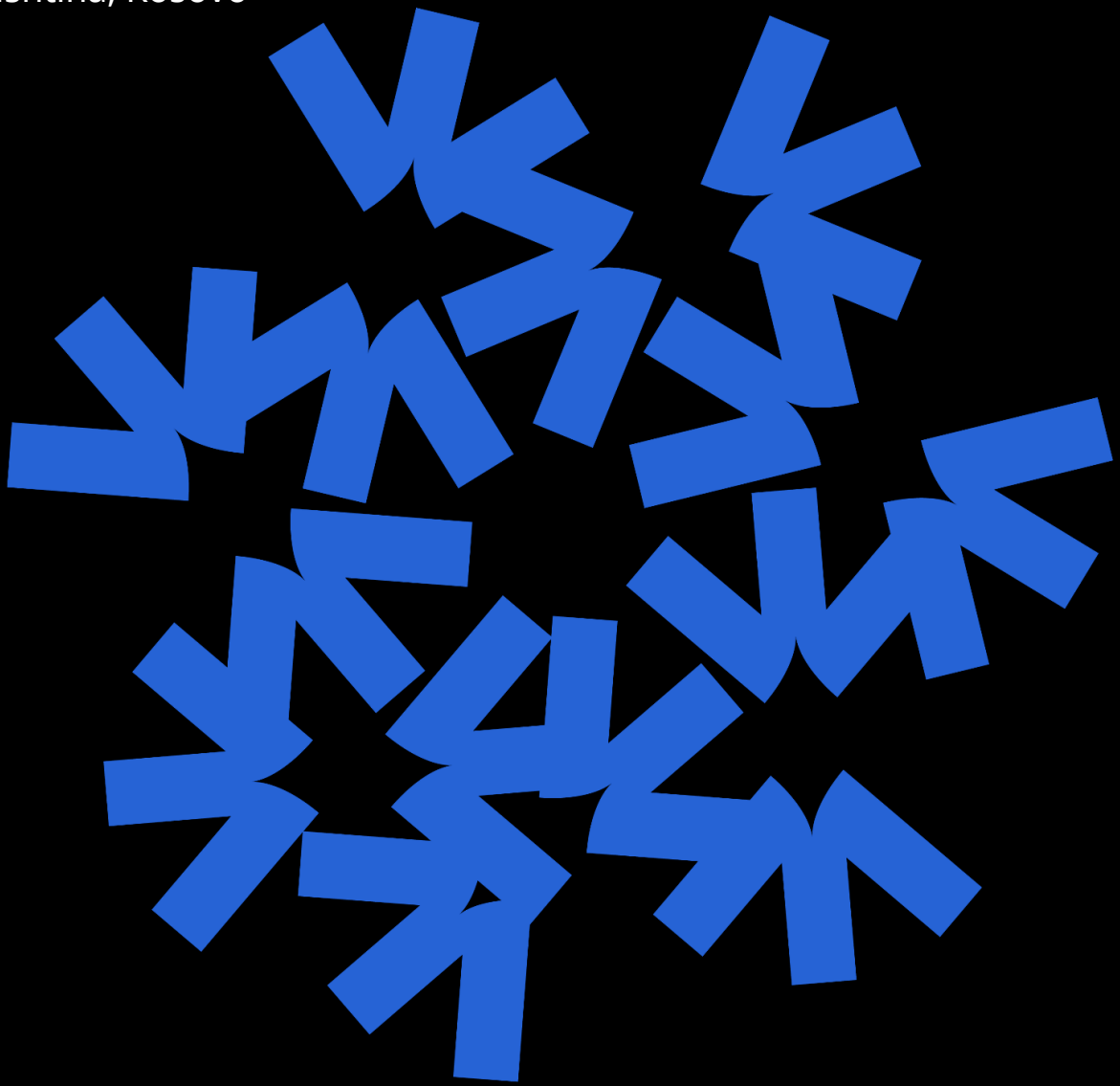
Integration of the Six Countries of the Western Balkans (WB6) in the European Union Agency for Cybersecurity

Policy Brief

September 22, 2024

Prishtina, Kosovo



KCSS
Kosovar Centre for Security Studies

Ignita
Igniting Collaboration

OPEN SOCIETY
FOUNDATIONS
WESTERN BALKANS

DISCLAIMER:

This report is produced by Kosovar Centre for Security Studies (KCSS) in the framework of the IGNITA initiative, funded by Open Society Foundations—Western Balkans.

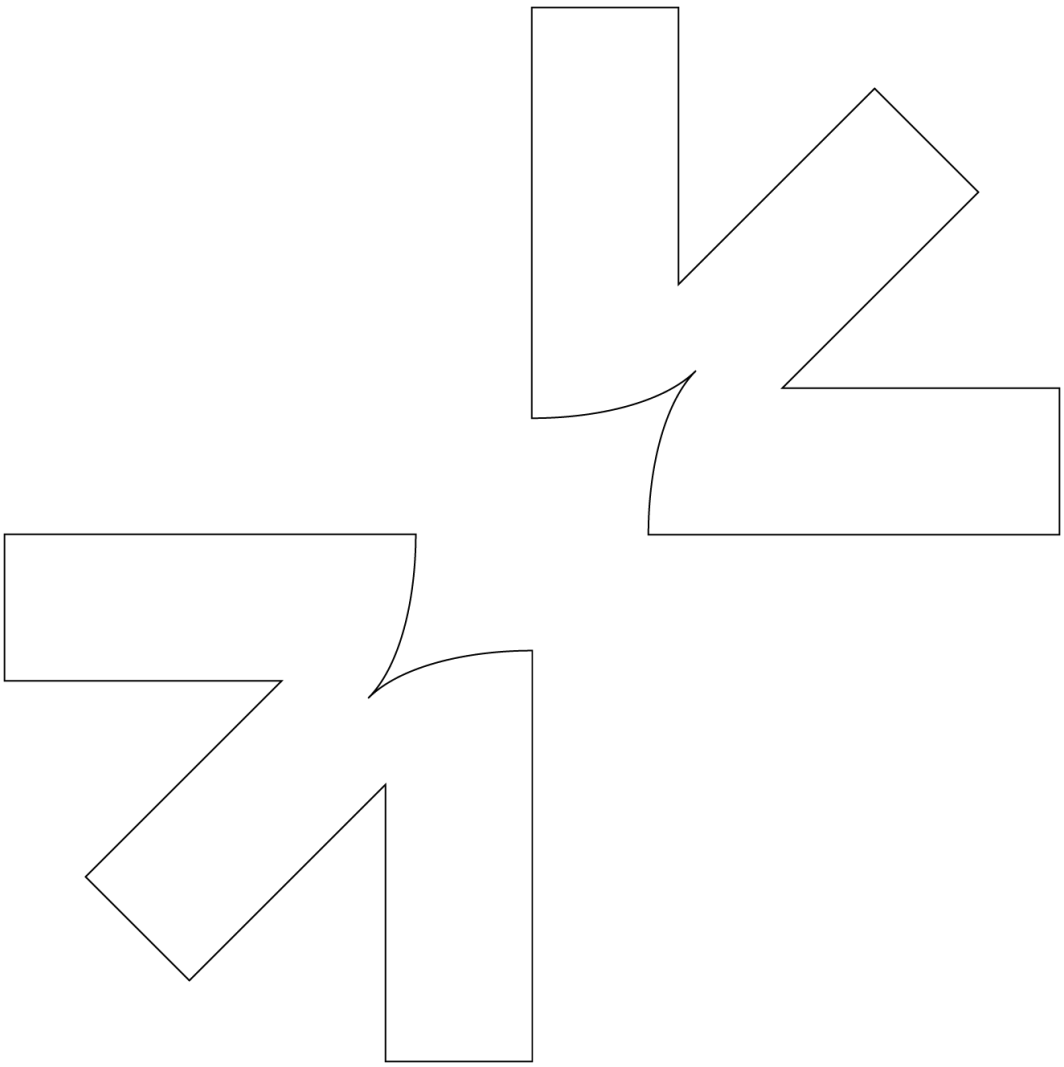


Table of Contents

.....1
List of Abbreviations and Acronyms 4
Introduction 5
Background on the European Union Cybersecurity Agency 6
On the EU Cybersecurity Act in General 6
European Union Cybersecurity Agency 9
European Cybersecurity Certification Framework 20
Integration of WB6 Countries into the European Union Cybersecurity Agency: State of Play..... 29
Albania 30
Bosnia and Herzegovina 31
Kosovo..... 31
Montenegro 32
North Macedonia..... 32
Serbia 33
Integration of WB6 Countries into the European Union Cybersecurity Agency: A Proposed Roadmap..... 33
What reforms need to be prioritised by WB6 for gradual integration into ENISA? 34
What options are available for gradual integration in ENISA of the WB6? 37
What WB6 countries need to do for gradual integration in ENISA?..... 38

List of Abbreviations and Acronyms

CAB	Conformity assessment body
CERT/CSIRT	Cybersecurity Emergency Response Team (*at national level*) / Computer Security Incident Response Team
CERT-EU	EU Cybersecurity Emergency Response Team
CoE	Council of Europe
CSA	Conformity self-assessment
DSM	Digital Single Market
EC	European Commission
ECCAC	EU cybersecurity conformity assessment certificate
ECC	EU cybersecurity certificate
ECCF	European Cybersecurity Certification Framework
ECCG	European Cybersecurity Certification Group
ECCS	European cybersecurity certification scheme
EAG	ENISA Advisory Group
EEA	European Economic Area
EEB	ENISA Executive Board
EED	ENISA Executive Director
EMB	ENISA Management Board
ENISA	European Union Agency for Cybersecurity (est. *European Network and Information Security Agency*)
ESoC	EU statement of conformity
EU	European Union
ICT	Information and communications technology
MS	Member State
NCCA	National cybersecurity certification authority
NCCS	National cybersecurity certification scheme
NCCF	National Cybersecurity Certification Framework
NLO	ENISA National Liaison Officers
OLAF	EU Anti-Fraud Office
RGF	EU Reform and Growth Facility for the Western Balkans
SCCG	Stakeholder Cybersecurity Certification Group
WB6	Six countries of the Western Balkans (*Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia*)

Introduction

The six Western Balkans countries (WB6) – Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia – are implementing their European Union accession reforms in a rather slow pace, with no vision on membership as the endpoint. On EU's side there lacks consensus among member states on membership of WB6, including because they their publics' are against further enlargement of the EU and the EU institutional system is inadequate to accommodate more member states into the already hyper-complex decision-making. While this state of affairs is a disincentive for EU accession reforms in WB6 countries, there are efforts to keep this reform process alive.

One such an effort in place for a decade now is the 'Berlin Process', a framework established by Germany to support the entire region to prepare for EU membership by promoting political cooperation, economic convergence and institutional reforms. Another approach that is gaining attention – particularly among civil society organisations in the region that are actively supporting the EU integration process – is that of phased accession. This approach would support WB6 countries in attaining EU standards by granting them access to EU mechanisms in specific policy areas in parallel with reforms they implement. This would be implemented in practice by allowing WB6 countries' institutions and other stakeholders dealing with specific policy areas to engage directly with their peers in the EU in an institutional learning process. EU agencies are typical such mechanisms. They are EU-level institutions specialized in specific policy area that exercise regulatory functions. In this role they drive through expertise – together with the European Commission (which also conducts membership negotiations with WB6 countries) – the EU acquis development in their policy areas. They also guide and support implementation and enforcement of the acquis and are involved in overseeing this.

Rule of law as a component of governance that includes several policy areas is a priority pillar for EU accession, and thus also part of the Cluster 1 (on Fundamentals) of EU membership negotiations in the recently introduced 'enhanced enlargement methodology'. Moreover, for WB6 countries digitalisation is a crosscutting area that is important for both domestic governance and as a priority area in their EU accession reforms, and as such affects all policy areas. An EU agency operating in the nexus between rule of law and digitalisation is the European Agency for Cybersecurity (ENISA). Therefore, establishing cooperation with it, with a view to advancing to some form of membership and then to full membership – in parallel with their advancement of EU accession process to full membership – is critical for the development of WB6 countries' institutional capacities for cybersecurity. This would also be useful to guide them in implementing EU accession reforms in this area. Thirdly, this would support them in their ongoing efforts to counter cybercrime and cyber incidents.

The policy brief discusses integration of WB6 countries into the EU Agency for Cybersecurity. It consists of three section. The first section provides a background on ENISA, focusing on two aspects: (1) the EU Cybersecurity Act as the acquis act regulating ENISA and cybersecurity as a policy area, and (2) ENISA's internal organisation and functioning, as well as the European cybersecurity certification framework as the EU-level regulatory mechanism in place for

cybersecurity. The second section discusses the area of cybersecurity in each WB6 country, focusing on the state of play with regard to legislation, policies and institutional framework, as well as on key EU-driven reform priorities. The final section puts forward a list of reform priorities that need to be pursued for phased accession of WB6 countries into ENISA.

Background on the European Union Cybersecurity Agency

The European Union Agency for Cybersecurity (ENISA) was established in 2004 and functions since then. It was initially established with a time-limited term and provisional mandate to regulate, at the EU level, cybersecurity as an emerging policy area. This regulatory function, established by the EU Cybersecurity Act, aims to achieve a high level of cybersecurity across the Union and to tackle fragmentation of the EU digital single market from the aspect of cybersecurity. This section discusses the EU Cybersecurity Act, ENISA as the EU-level institutional setup in charge of cybersecurity, and the European cybersecurity certification framework as the instrument ENISA it is equipped with to exercise its functions.

On the EU Cybersecurity Act in General

ENISA is the European Union (EU) agency specialized in the area of cybersecurity. Its mission is to achieve a common high level of cybersecurity across the Union. It achieves this mission by contributing to EU cyber policy; enhancing trustworthiness of ICT products, services and processes with European cybersecurity certification schemes (ECCSs); cooperating with Member States (MSs) and EU bodies; and helping the EU prepare for future cyber challenges.[1] Its headquarters is in Athens, and it also has an office in Heraklion, on the island of Crete, and one in Brussels.[2]

It was established in 2004 as the European Network and Information Security Agency (ENISA) through the Regulation (EC) No. 460/2004 of 10 March 2004 establishing this agency.[3] This regulation established ENISA for an initial mandate of five years[4], afterwards extended three more times through amendments to this regulation that were adopted in

[1] *ENISA, ENISA Mandate and Regulatory Framework, https://www.enisa.europa.eu/about-enisa/regulatory-framework.*
[2] *ENISA, ENISA – Contact, https://www.enisa.europa.eu/about-enisa/contact.*
[3] *EUR-Lex – Official Gazette of the European Union,* ***Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency,*** *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.*
[4] *Ibid, Article 27.*

2008[5], 2011[6] and 2013[7], and finally became a permanent agency through the Regulation 2019/881 (that was adopted on 17 April 2019 and entered into force in 7 May 2019)[8], known as the EU Cybersecurity Act. The EU Cybersecurity Act also changed the name of this Agency from 'European Network and Information Security Agency' to 'EU Agency for Cybersecurity'.

The EU Cybersecurity Act contains 69 articles, structured as follows: *Title I* (Art. 1-2), *general provisions*, on the subject matter and scope of this regulation; *Title II* (Art. 3-45), on mandate and organisation of ENISA; *Title 3* (Art. 46-65), on the *European cybersecurity certification framework* (ECCF); and *Title 4* (Art. 66-69), *final provisions*. It also contains an *annex* of requirements to be met by cybersecurity conformity assessment bodies (CABs). The tile on ***general provisions***[9] covers the scope and purpose of the EU Cybersecurity Act and definitions. In terms of its scope, it sets ENISA's objectives, tasks and internal organisation; and ECCF. In other words, it governs the institutional framework and European standards in the area of cybersecurity. While it is directly applicable in EU member states, integration of WB6 countries into ENISA and reaching these standards set by the EU Cybersecurity Act requires them to implement reforms to align their domestic legislation with it and to implement and enforce it. The main definitions of this act that are relevant for this policy brief are the following:

- *National strategy on the security of network and information systems* is the policy document providing strategic objectives and priorities on security of network and information systems at the national level;
- *Operator of essential services* is a public or private entity providing services that are essential for the maintenance of critical societal and/or economic activities whose provision depends on network information systems and if an incident on such systems would have disruptive effects on the provision of such services;
- *European cybersecurity certification scheme* is a document issued by a relevant body, attesting that a given ICT product, service or process has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;

[5] *EUR-Lex – Official Gazette of the European Union, Regulation (EC) No. 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:293:0001:0002:EN:PDF.*

[6] *EUR-Lex – Official Gazette of the European Union, Regulation (EC) No. 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No. 460/2004 establishing the European Network and Information Security Agency as regards its duration, https://www.enisa.europa.eu/media/news-items/extension-of-enisa2019s-mandate-published-1.*

[7] *EUR-Lex – Official Gazette of the European Union, Regulation (EU) No. 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN.*

[8] *EUR-Lex – Official Gazette of the European Union, Regulation (EU) No. 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881.*

[9] Ibid, Art. 1-2.

- *National cybersecurity certification scheme* (NCCS) is a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, services and processes falling under the scope of the specific scheme;
- *European cybersecurity certificate* (ECC) is a document issued by a relevant body attesting that a given ICT product, service or process has been evaluated for compliance with specific security requirements laid down in an EU cybersecurity certification scheme;
- *Accreditation* is an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity;
- *National accreditation body* is the sole body in a MS that performs accreditation with authority derived from the State;
- *Conformity assessment* is the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled;
- *Conformity assessment body* is a body that performs conformity assessment activities including calibration, testing, certification and inspection;
- *Conformity self-assessment* is an action carried out by a manufacturer or provider of ICT products, services or processes which evaluates whether they meet the requirements of a specific EU cybersecurity certification scheme;
- *Assurance level* is a basis for confidence that an ICT product, service or process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which they have been evaluated but as such does not measure their security.

The list of *essential services*[10] is established at the EU level by the EU Directive 2016/1148 on security of network and information systems, specifically its Article 4, paragraph 4, and further detailed in Annex II. It includes services in the following seven areas:

- Energy:
  - Electricity;
  - Oil; and
  - Gas;
- Transport:
  - Air transport;
  - Rail transport;

[10] *EUR-Lex – Official Gazette of the European Union, 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, Art. 4 (4), Annex I, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148.*

  - Water transport; and
  - Road transport;
- Banking;
  - Financial market infrastructures;
- Health sector, specifically health care settings (including hospitals and private clinics);
- Drinking water supply and distribution; and
- Digital infrastructure.

Provisions of the EU Cybersecurity Act on ENISA specifically focus on its mandate, including legal status, objectives and tasks; its internal organisation, including budget and financial rules, key staff and their tasks and responsibilities and capacity-building; operational cooperation at EU level and international cooperation; aspects related to the market and standards; information, public awareness and education; research and innovation; its internal planning instrument; and rules related to institutional interests, confidentiality, access to information and personal data protection.

European Union Cybersecurity Agency

The title of the EU Cybersecurity Act on ***ENISA*** covers three aspects: its mandate, its internal organisation and cooperation with third countries and international organisations.
ENISA's mandate: The EU Cybersecurity Act mandates ENISA to achieve a common high level of cybersecurity within the EU, including by supporting MSs and EU institutional actors, thus contributing to reducing fragmentation of the EU internal market in this area. It achieves this by serving as a reference point for advice and expertise on cybersecurity for EU institutional actors and other EU stakeholders. As an expertise-based Union agency, ENISA carries out functions given to it by EU law that sets out cybersecurity measures that are binding across the EU and in all MSs. It complements MSs' functions in this regard, i.e. has to avoid duplicating them, and takes into consideration their existing expertise.

ENISA functions independently, with its own budgetary and human resources. It also has legal personality with extensive legal capacity under national law.[11] In other words, seen in the context of the EU-wide cybersecurity landscape, ENISA's specialized functions take place at two levels of intervention: policy development; and implementation and enforcement:
ENISA contributes to *policy development* in the area of cybersecurity through the following functions:

- Provision of expertise and advice to EU and MSs' institutions in charge of cybersecurity, including best practices and recommendations that are useful for the development of legislation and policies in this area;

[11] *EUR-Lex – Official Gazette of the European Union, Regulation (EU) No. 2019/881 (Cybersecurity Act), Art. 3.*

- Supporting EU-level reforms in the legislation, such as NIS2 Directive, and policies in this area;
- Supporting institutional capacity building in MSs by providing training and facilitating knowledge sharing, including for the purpose of development of national cybersecurity strategies;
- Conducting threat and risk analysis to inform stakeholders on current and emerging cybersecurity risks, threats and vulnerabilities, including by publishing reports and assessments, with a view to supporting them to tackle such risks through legislation and policies;
- Supporting research and innovation on new trends and technological developments in the EU market and facilitating cooperation among researchers, industry and EU and MSs' institutions, thus contributing to the development of legislation and policies for the EU-wide, cybersecurity landscape and promoting them;

ENISA contributes to implementation and enforcement in the area of cybersecurity through the following functions:

- Provision of expertise and advice to EU and MSs' institutions in charge of cybersecurity, as well as to businesses as market players through practices, recommendations and technical solutions to address emerging cyber threats;
- Supporting implementation and enforcement of EU legislation, such as the NIS II Directive, and policies in this area,
- Supporting institutional capacity building in MSs by providing training and facilitating knowledge sharing, including for the purpose of enhancing skills of cybersecurity professionals;
- Supporting MSs in managing and responding to cybersecurity incidents by facilitating coordination between national Computer Security Incident Response Teams (CSIRTs) and assisting MSs in developing mechanisms and technical working tools for this purpose;
- Supporting cooperation and networking among relevant stakeholders across the EU, with a view to ensuring sustained sharing of information and best practices;
- Promoting cybersecurity awareness and education among the business community and other stakeholders, as well as the general public across the EU.

The EU Cybersecurity Act sets *objectives*[12] for ENISA to fulfil its specialized mandate in the area of cybersecurity, namely to:

- Serve as a centre of expertise;
- Assist EU institutions and MSs in developing and implementing EU policies;
- Support capacity-building and preparedness across the EU;

[12] *Ibid, Art. 4.*

- Promote cooperation at EU level and among MSs, including with private stakeholders;
- Contribute to increasing cybersecurity capabilities in order to support MSs' actions in preventing and responding to cyber threats;
- Promote the use of EU cybersecurity certification, with a view to avoiding the fragmentation of the internal market; and
- Promote a high level of public awareness across the board in the EU.

In order to achieve these objectives, ENISA's *tasks*[13] are organized into eight pillars: development and implementation of EU policy and law; capacity-building; EU-level operational cooperation; market, cybersecurity certification and standardization; knowledge and information; awareness-raising and education; research and innovation; and international cooperation.Under the *development and implementation of EU cybersecurity policy and law* pillar, it is tasked to:

- Assist and advise on their development and review, through independent opinions, analysis and preparatory work; and assist MSs and EU institutions in developing and promoting them;
- Assist MSs to implement them consistently, through opinions, guidelines, advice and exchange of best practices;
- Support: (a) development and implementation of EU policy on electronic identity and trust services, through advice, technical guidelines and exchange of best practices; (b) promotion of security of electronic communications, through advice, expertise and exchange of best practices; and (c) MSs in implementing specific aspects of EU policy and law relating to data protection and privacy, through advice to the European Data Protection Board upon request; and
- Contribute to the work of the Cooperation Group established through Directive (EU) 2016/1148 through expertise and assistance.

Under the *cybersecurity capacity-building* pillar, it is tasked to:

- Assist MSs and EU institutions in the prevention, detection and analysis of, and capabilities to respond to, cyber threats and incidents, through provision of knowledge and expertise and of appropriate support to the EU Cybersecurity Emergency Response Team (CERT-EU);
- Assist MSs and EU institutions in establishing and implementing vulnerability disclosure policies on voluntary basis;
- Assist MSs, upon request, in developing national CSIRTs;
- Assist MS's and EU CSIRTs in raising the level of their capabilities, including by promoting dialogue and information exchange, with a view to ensuring that they possess a common set of minimum capabilities and operate according to best practices;

[13] *Ibid, Art. 5-12.*

- Assist MSs, upon request, in developing national security of network and information systems strategies and promote their dissemination, and follow their implementation in order to promote best practices;
- Assist EU institutions in developing and reviewing EU cybersecurity-related strategies, promoting their dissemination and tracking their implementation;
- Assist MSs through regular EU level cybersecurity exercises and policy recommendations based on evaluation of such exercises;
- Assist relevant public bodies through training on cybersecurity, in cooperation with stakeholders, as appropriate;
- Assist the ENISA Cooperation Group in the exchange of risks and incidents related best practices, particularly with regard to identification by MSs of operators of essential services, including on cross-border dependencies;
- Support sector-specific information sharing, in particular in those of essential services, through best practices and guidance on available tools and procedures and on addressing regulatory issues related to information-sharing.

Under the cybersecurity operational cooperation at the EU level pillar, it is tasked to:

- Support operational cooperation among MSs, EU institutions and between stakeholders;
- Cooperate and establish synergies with EU institutions, including CERT-EU, with related services and supervisory authorities dealing with protection of privacy and personal data, to address issues of common concern, including through exchange of know-how and best practices, advice and guidelines, and establishment of practical arrangements to execute specific tasks;
- Serve as CSIRTs network secretariat and thus support information sharing and cooperation;
- Support MSs, upon request, in operational cooperation within the CSIRTs network, through advice to improve their capabilities to prevent, detect and respond to incidents and in relation to specific cyber threats; assistance to assess incidents with a significant or substantial impact (by providing expertise, facilitating their handling and supporting voluntary sharing of information and technical solutions between MSs); by analysing vulnerabilities and incidents based on publicly available and voluntarily shared information by MSs; and support in relation to ex-post technical inquiries regarding incidents with a significant or substantial impact;
- Organise regular cybersecurity exercises at EU level and support MSs and EU institutions, upon request, in organising them (including organising a large-scale comprehensive one and helping to organise sectoral ones together with relevant organisations);
- Prepare a regular in-depth EU Cybersecurity Technical Situation Report on cyber incidents and cyber threats, in cooperation with MSs, based on publicly available information, its analysis and reports shared by MSs, their CSIRTs or the single points of contacts; and

- Contribute to developing a cooperative response at EU and MSs' level (upon MSs' request) to large-scale cybersecurity-related cross-border incidents or crises, by aggregating and analysing reports from MS sources contributing to public awareness; ensuring efficient flow of information and providing escalation mechanisms between the CSIRTs network and EU-level decision-makers; facilitating technical handling of them in MSs' (including by supporting sharing of such solutions); supporting EU institutions and MSs in public communication; and testing EU-level response cooperation plans and supporting MSs in testing them at the national level.

Under the market, cybersecurity certification, and standardization pillar, it is tasked to:

- Support and promote development and implementation of the EU policy on certification of ICT products, services and processes, through monitoring standardisation-related developments and recommendation of appropriate technical specifications for schemes with no standards available; preparation of candidate certification schemes; evaluation of EU certification schemes and taking part in peer reviews in MSs at least every five years; and assistance to the EC as secretariat to the European Cybersecurity Certification Group (ECCG) established by this Act;
- Act as secretariat to the Stakeholder Cybersecurity Certification Group (SCCG) established by the EU Cybersecurity Act;
- Compile and publish guidelines and develop good practices on cybersecurity requirements for ICT products, services and processes, in cooperation with national certification authorities and the industry, in a formal, structured and transparent way;
- Contribute to capacity-building related to evaluation and certification through guidelines and support to MSs at their request;
- Facilitate the establishment and take-up of EU and international risk management and security standards for ICT products, services and processes;
- Draw up advice and guidelines, in cooperation with MSs and the industry, in technical areas related to security requirements for operators of essential services and digital service providers, and regarding already existing standards, including MSs' ones; and
- Perform and disseminate regular market trends analyses, with a view to fostering the EU digital single market.

Under the *cybersecurity knowledge and information* pillar, it is tasked to:

- Perform analyses of emerging technologies and provide topic-specific assessments on expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity;
- Perform long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents;

- Provide advice, guidance and best practices, in cooperation with experts from MSs authorities and relevant stakeholders, for the security of network and information systems, particular for the infrastructure and providers of digital services in the essential services sectors listed in Annex II;
- Pool, organise and make available to the public information on cybersecurity provided by EU institutions, MSs and private and public stakeholders; and
- Collect and analyse publicly available information on significant incidents and compile reports, to provide guidance to citizens, organisations and businesses across the EU, through a webpage.

Under the *cybersecurity awareness-raising and education* pillar, it is tasked to:

- Raise public awareness of risks and provide guidance on good practices for individual users aimed at citizens, organisations and businesses, including cyber-hygiene and cyber-literacy;
- Organise regular outreach campaigns, in cooperation with MSs and EU institutions, to increase cybersecurity and its visibility in the EU and encourage a broad public debate;
- Assist MSs in efforts to raise awareness and promote education; and
- Support coordination and exchange of best practices among MSs on awareness and education.

Under the *cybersecurity research and innovation* pillar, it is tasked to:

- Advise EU institutions and MSs on research needs and priorities, to enable effective responses to current and emerging risks and cyber threats, including with respect to new and emerging ICT and to using risk-prevention technologies effectively;
- Participate in implementation of research and innovation funding programmes, within powers conferred by the EC or as a beneficiary; and
- Contribute to the EU-level strategic research and innovation agenda in the area of cybersecurity.

Under the *cybersecurity international cooperation* pillar, it is tasked to contribute to EU's efforts to cooperate with third countries, international organisations and to promote international cooperation within relevant international cooperation frameworks, by:

- Engaging as an observer in the organisation of international exercises, and analysing and reporting to the Management Board on their outcome;
- Facilitating the exchange of best practices, upon EC's request;
- Providing the EC with expertise, upon its request; and
- Providing advice and support to the EC on matters concerning agreements for mutual recognition of cybersecurity certificates with third countries, in cooperation with ECCG.

The EU Cybersecurity Act obliges the EC to carry out an ***evaluation*** of ENISA, every five years following its entry into force, focusing on three aspects: Agency's impact, effectiveness, efficiency and working practices; the ECCF's objective of ensuring an adequate level of cybersecurity of ICT products, services and processes in the EU and improving functioning of the internal market; and whether essential cybersecurity requirements for access to the EU market are necessary to prevent ICT products, services and processes that do not meet them from entering it. The evaluation report with conclusions should be transmitted by the EC to the EP, the Council and to ENISA Management Board, and made public. Based on its findings, the EC may propose to amend the EU Cybersecurity Act's provisions related to ENISA.[14]

ENISA's internal organisation[15]***:*** The EU Cybersecurity Act establishes the following structures of ENISA: Management Board (EMB), Executive Board (EEB), Executive Director (EED), Advisory Group (EAG) and the National Liaison Officers (NLO) Network. A description of each of these structures in simpler practical terms is provided in the ENISA's official webpage.[16]

The *Management Board* (EMB) is the highest governing body of ENISA. It consists of one member appointed by each MS and two by the EC (all of them with alternates) for renewable four-year terms. They are appointed on the basis of their knowledge in the field of cybersecurity (also aiming at gender balance) and have one vote each. This Board appoints its Chairperson and the Deputy Chairperson from among its members, by two-thirds of the vote, for a once-renewable four-year term, and takes decisions by simple majority. EMB's current membership consist of two EC representatives and those from 25 MSs (with appointments by two of them pending). In addition, three countries of the European Economic Area (EEA) – Iceland, Lichtenstein and Norway – are also represented as observer members. All members also have their alternates.[17] EMB is currently chaired by the representative of Germany.[18]

The *Executive Board* (EEB) assists the Management Board (EMB) in its work. It prepares decisions to be adopted by the EMB, ensures (together with this board) adequate follow-up of findings and recommendations of the EU Anti-Fraud Office (OLAF) investigations and other audit reports and evaluations, and assists the Executive Director (EED) in implementing EMB's decisions on administrative and budgetary matters. EEB is composed of five members appointed from among EMB members for renewable four-year terms. One

[14] *Ibid, Art. 67.*
[15] *Ibid, Art. 13-23.*
[16] *ENISA, Structure and Organisation, https://www.enisa.europa.eu/about-enisa/structure-organization.*
[17] *ENISA, List of ENISA Management Board Representatives and Alternates, https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/MBMemberAlternate.pdf.*
[18] *ENISA, Executive Board Representatives and Alternates, https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/list-of-enisa-executive-board-representatives-and-alternates.pdf.*

of them, who may also chair it, is the EMB Chairperson, and another is an EC member. The EED also attends EEB meetings, but has no right to vote. EEB is currently chaired by the representative of Germany, as well.[19]

The *Executive Director*[20] is ENISA's top management authority. He/she is independent in the performance of his/her duties, accountable to the Management Board, and also reports to the EP and the Council, upon request. This position is currently held by **Juhan Lepassaar from Estonia, as of October 2019.**[21]

Functions of the Management Board (EMB) and responsibilities of the Executive Director (EED) are the following:

- EMB appoints the Executive Director, extends his/her term of office and may dismiss him/her, all by two-thirds of votes of all its members, and he/she is accountable to EMB;
- EMB establishes ENISA's general direction, ensuring legality and consistency, while EED administers it on daily basis and implements EMB's decisions;
- EED prepares ENISA's single programming document and implements it, while EMB adopts it by two-thirds of votes, taking into account EC's opinion, and supervises its implementation;
- EED prepares the annual report on ENISA's activities, while EMB assesses and approves it, and then submits it to EP, the Council, EC and the Court of Auditors, and makes it public;
- EED prepares ENISA's draft statement of estimates of revenue and expenditure and implements its annual budget and financial rules, while EMB adopts the budget and financial rules (by two-thirds of votes of all members), the latter after consulting the EC, and exercises related functions;
- EED prepares an anti-fraud strategy for ENISA, while EMB adopts it, having regard to a cost-benefit analysis of measures to be implemented;
- EED also protects EU's financial interests through various measures against fraud, corruption and illegal activities in ENISA's functioning;
- EED prepares an action plan to follow-up on conclusions and recommendations of evaluations and reports to the EC on its implementation, while EMB adopts it and ensures follow-up;
- EED prepares an action plan to follow-up on internal and external audit reports and evaluations and on OLAF investigations and reports to the EC and EMB on its implementation, while EMB adopts it and ensures adequate follow-up;
- EMB adopts rules for the prevention and management of conflict of interest in respect of its members and its own rules of procedure;

[19] *Ibid.*
[20] *EUR-Lex – Official Gazette of the European Union, Regulation (EU) No. 2019/881 (Cybersecurity Act), Art. 20, 15.*
[21] *ENISA, ENISA Executive Director, https://www.enisa.europa.eu/about-enisa/structure-organization/executive-director.*

- EMB takes decisions related to establishment and modification of ENISA's internal structures, adopts and implements its staffing rules and appoints an independent accounting officer;
- EMB authorises the establishment of working arrangements on cooperation at EU level and with third countries and international organisations;
- EED maintains contact with the business community and consumer organisations, and regularly exchanges views and information with EU institutions on cybersecurity, to ensure coherence in EU's policy;
- EED may also set up ad hoc working groups composed of experts, including from MSs' competent authorities (and informs EMB on this), regulated by ENISA's internal rules of operation; and may establish local offices in MSs (upon their prior consent).

The EU Cybersecurity Act has also established two advisory bodies for ENISA: Advisory Group (EAG) and Stakeholder Cybersecurity Certification Group (SCCG). It also establishes the National Liaison Officers (NLO) Network.

Advisory Group's (EAG) role focuses on ENISA's actual work, particularly advising the EED on its annual work programme and on ensuring communication with relevant stakeholders related to it. It is composed of recognised experts representing stakeholders, such as the ICT industry, providers of electronic communications networks or services, SMEs, essential service operators, consumer groups, academics, representatives of competent authorities and of European standardisation organisations, as well as of law enforcement and data protection supervisory authorities. It is chaired by the EED and its members are proposed by him/her and selected by the EMB for a term of two and a half years each. EC and MS experts and representatives of other (non-member) bodies may also participate in its work. It regularly informs the EMB on its activities. Detailed rules are specified by ENISA's internal rules. Currently EAG has as its members 33 experts (19 experts as reserve members) and has invited eight organisations to appoint members representing them. They are appointed through EMB decision for a period until 2025[22]

The role of the *Stakeholder Cybersecurity Certification Group* (SCCG) focuses on ECCF, i.e. to advise the EC on strategic issues regarding it, as well as to assist it in the preparation of EU's European cybersecurity certification rolling work programme, issue an opinion on it, and (in urgent cases) advise it and ECCG on the need for additional certification schemes. It also advises ENISA, upon request, on general and strategic matters in its tasks relating to market, cybersecurity certification, and standardisation. It is composed of members selected from among recognised experts representing the relevant stakeholders. They are

[22] *ENISA, Decision of ENISA Management Board setting up and Advisory Group for the period 2023-2025, https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2023-02-setting-up-enisa-advisory-group-for-period-2023-2025.pdf.*

selected by the EC following a transparent and open call and on the basis of a proposal from ENISA. It is co-chaired by EC's and ENISA's representatives.

The *NLO Network* facilitates information exchange between ENISA and MSs; supports it in disseminating its activities, findings and recommendations to relevant stakeholders; and acts as a point of contact at national level to facilitate cooperation between ENISA and national experts for implementation of its annual work programme. It is set up by ENISA Management Board, acting on a proposal by the Executive Director, and is composed of one representative of each MS (NLOs), appointed by them. This network currently consists of representatives of 29 states (the 27 EU MSs and Lichtenstein and Norway), with nine states having two representatives each and the rest one representative each.[23]

The EU Cybersecurity Act also regulates the following aspects of ENISA's internal functioning: its budget and financial rules; staff; the single programming document; prevention of conflict of interest and anti-fraud, as well as transparency, confidentiality, access to documents and protection of personal data.

On the *budget and financial rules*[24], this act lays down procedural steps and institutional responsibilities for determining and approving ENISA's budget and financial rules (described above), and the structure and implementation of the budget. ENISA draws its budget from five sources: contributions from the general EU budget, revenues assigned to specific expenditure items, EU funding in the form of delegation agreements or *ad hoc* grants, contributions from third countries participating in its work, and voluntary contributions from MSs. ENISA's financial regulation and annual budgets and accounts are published on its official webpage.[25]

Staff-related provisions[26] cover ENISA staff's privileges and immunity, its Executive Director, and seconded national experts and other staff. EU treaty provisions on privileges and immunity apply for ENISA staff as well. The Executive Director is appointed by the Management Board from a list of candidates proposed by the EC, for a term of five years that may be extended, and also directly contracted by its Chairperson. This Board also decides on the extension of the term of office or removal from office, taking into account the end-term assessment that is conducted by the EC. The EU Cybersecurity Act also allows ENISA to make use of seconded national experts or other staff not employed by it, but the EU Regulations of Officials and the Conditions of Employment of Other Servants shall not apply to them.

[23] *ENISA, List of ENISA National Liaison Officers (NLO), https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/list-of-enisa-national-liaison-officers.*
[24] *EUR-Lex – Official Gazette of the European Union, Regulation (EU) No. 2019/881 (Cybersecurity Act), Art. 29-32.*
[25] *ENISA, Accounting and Finance, https://www.enisa.europa.eu/about-enisa/accounting-finance.*
[26] *EUR-Lex – Official Gazette of the European Union, Regulation (EU) No. 2019/881 (Cybersecurity Act), Art. 35-37.*

As its integrated planning framework, ENISA's *single programming document*[27] is also the basis to plan its work in multiannual and annual work programmes, including activities and financial and human resources to implement it. The multiannual work programme is strategic programming, setting objectives, expected results and performance indicators, while annual one contains detailed objectives and expected results, performance indicators, as well as a description of actions to be financed and an indication of resources allocated. While strategic programming is updated when appropriate, in particular where necessary to address the outcome of the evaluation, resource programming is updated annually. The current single programming document covers the 2024-2026 period.[28]

On *prevention of conflict of interest and anti-fraud*[29], the EU Cybersecurity Act provides the legal basis for the EU Court of Auditors and OLAF to audit, respectively investigate ENISA's work for potential fraud corruption or other illegal activities affecting EU's financial interests. These provisions also cover all grant beneficiaries, contractors and subcontractors, and are also binding in the context of ENISA's cooperation with third countries and international organisations.

The EU Cybersecurity Act stipulates that standards of transparency, *confidentiality, access to documents and protection of personal data*[30] are binding for ENISA, and it is obliged to adopt internal rules and practical arrangements to implement them (optional in the case of data protection). Transparency is ensured through access to public documents and direct observance of its activities by interested parties (the latter authorised by the Management Board, upon Executive Director's proposal). In order to prevent conflict of interest and protect its independence ENISA is also obliged to publish declarations of interest of members of the Management Board, the Executive Director, officials seconded by MSs and external experts engaged in its work. All ENISA's staff, current or past, is obliged to comply with treaty confidentiality provisions, and thus prohibited from sharing with third party information processed or received in relation to which a reasoned request for confidential treatment has been made. Access to documents means that ENISA decisions may be the subject of a complaint to the European Ombudsman or legal action before the EU Court of Justice if access to public documents it holds is not allowed within fifteen working days. Lastly, ENISA is also legally bound by the EU Regulation (EU) 2018/1725 on protection of personal data, and may also adopt additional measures to comply with it.

Cooperation with third countries and international organisations, and international cooperation[31]***:*** The EU Cybersecurity Act contains provisions on cooperation of ENISA with third countries, international organisations and within relevant international cooperation frameworks. They provide for ENISA to establish working arrangements with such entities,

[27] *Ibid, Art. 24.*
[28] *ENISA, ENISA Single Programming Document 2024-2026, https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2024-2026.*
[29] *EUR-Lex – Official Gazette of the European Union, Regulation (EU) No. 2019/881 (Cybersecurity Act), Art. 25, 33.*
[30] *Ibid, Art. 26-28, 41.*
[31] *Ibid, Art. 12, 42.*

upon EC's prior approval, but do not create legal obligations for the EU and its MSs as legal entities. The aim of such cooperation is for ENISA to promote international cooperation between the EU and such entities on cybersecurity by engaging as an observer in the organisation of international exercises, facilitating the exchange of best practices, providing the EC with expertise, as well as by advising and supporting it on matters related to agreements for mutual recognition of cybersecurity certificates with third countries.

ENISA is also allowed to cooperate with third countries and international organisations that have concluded agreements with the EU to that effect. To that end, it may establish working arrangements regulating the nature, extent and manner their participation in its work and initiatives, as well as financial contributions and staff. In terms of procedures, the Management Board adopts a strategy for relations with third countries and international organisations under ENISA's remit while the EC concludes working arrangements with the ENISA Executive Director ensuring that the agency operates within its mandate and the existing institutional framework in the context of such cooperation.

These provisions constitute a legal basis for WB6 countries to engage in cooperation with ENISA. Given these countries' long-term ambition to become EU member states in the future and the importance of cybersecurity for them in this context, such cooperation needs to be established in sound legal grounds, and at the same time allow for advancement of formal relations with this agency from cooperation to membership. Taking this long-term view as the basis, it is also advisable that WB6 countries engage with ENISA not as all other third countries, but establish closer cooperation in parallel and upon fulfilment of specific preconditions required by the EU Cybersecurity Act and other relevant acquis.

A key incentive and driver for WB6 countries for cooperation with ENISA to be closer and long-term – that would ideally advance into membership in observer status, and then to full membership along the advancement of their EU membership path – is to promote and push forward their ongoing reforms in the area of cybersecurity. The practice of observer members is already applied by ENISA, with EEA countries of Iceland, Lichtenstein and Norway enjoying this status. Given ENISA's nature and mandate as an expertise-based institution, it would operationally engage in cooperation, once defined through legal instruments, with national cybersecurity agencies. As the institution that is legally mandated to lead, on EU's side and on its behalf, accession processes of each WB6 country – the EC would also be involved in such cooperation. Importantly, the nature, format and instruments of such cooperation need to be uniform with all these countries, and also based on the same preconditions.

European Cybersecurity Certification Framework

The title of the EU Cybersecurity Act on the ***European cybersecurity certification framework (ECCF)*** [32] covers three aspects: the setup; its content and governance; and correcting mechanisms enabling its functioning.

ECCF's setup: By establishing the ECCF, the EU Cybersecurity Act aims to set and implement unified high cybersecurity standards, that are compulsory across the EU, for ICT products, services and processes, also with a view to avoid fragmentation of the internal market in this area. Provisions under this aspect regulate the following: ECCF's purpose, the policy framework governing it, EU cybersecurity certification schemes' security objectives, the process to establish a new EU cybersecurity certification scheme or update an existing one, and a webpage as a single information hub on such schemes.

ECCF's purpose is to improve conditions of functioning of the EU internal market by increasing the level of cybersecurity and enabling a harmonised approach to cybersecurity certification schemes, with a view to creating a digital single market for ICT products, services and processes. To this end, ECCF is a mechanism to establish EU cybersecurity certification schemes and to attest that ICT products, services and processes evaluated thereby comply with security requirements set in order to protect availability, authenticity, integrity or confidentiality of respective data, functions or services.

The *policy framework* governing ECCF is the EU rolling programme, published by the EC and revised at least every three years, taking into account opinions by ECCG and SCCG. As an official EU policy document, it identifies strategic priorities for future EU cybersecurity certification schemes and a list of ICT products, services and processes that could benefit from such a scheme. An ICT product, service or process is included in this list if it meets the following criteria: availability of national cybersecurity certification schemes covering it (particularly regarding the risk of fragmentation) a relevant EU or MS law or policy, market demand, developments in the cyber threat landscape, and an ECCG request to prepare a candidate scheme.

An EU cybersecurity certification scheme should meet the following *security objectives:*

- Protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, service or process;
- Protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, service or process;
- Ensure that authorised persons, programmes or machines are able only to access data, services or functions to which their access rights refer;
- Identify and document known dependencies and vulnerabilities;

[32] *Ibid, Art. 46-65.*

- Record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- Make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- Verify that ICT products, services and processes do not contain known vulnerabilities;
- Restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;
- Make sure that ICT products, services and processes are secure by default and by design; and
- Make sure that ICT products, services and processes are provided with up-to-date software and hardware.

The EU Cybersecurity Act also lays out the following rules on *assurance levels* of an ECCS:

- It may specify one or more of three assurance levels for an ICT product, service and processes established (commensurate with the risk level associated with their intended use, in terms of the probability and impact of an incident):
    - Basic: ICT products, services and processes which an ECCS or EU statement of conformity (ESoC) is issued for meet basic security requirements, including security functionalities, and have been evaluated to minimise known basic risks of incidents and cyberattacks; evaluation activities at this level includes at least a review of technical documentation, or, if not appropriate, substitute evaluation activities with equivalent effect;
    - Substantial: ICT products, services and processes which an ECCS or ESoC is issued for meets the corresponding security requirements, including security functionalities, and have been evaluated at a level intended to minimise the known cybersecurity risks and the risk of incidents and cyberattacks carried out by actors with limited skills and resources; evaluation activities at this level includes at least a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that they correctly implement necessary security functionalities, or, if not appropriate, substitute evaluation activities with equivalent effect;
    - High: ICT products, services and processes which an ECCS or ESoC is issued for meet the corresponding security requirements, including security functionalities, and have been evaluated at a level intended to minimise the risk of state-of- the-art cyberattacks carried out by actors with significant skills and resources; evaluation activities at this level includes at least a review to demonstrate the absence of publicly known vulnerabilities, testing to demonstrate that they correctly implement the necessary security functionalities at the state of the art, and an assessment of their resistance to skilled attackers, using penetration testing;

- An ESoC also refers to any assurance level specified in the ECCS under which it is issued, as well as to related technical specifications, standards and procedures, including technical controls, to decrease the risk of or preventing cybersecurity incidents;
- Security requirements corresponding to each assurance level are provided in the relevant ECCS, including corresponding security functionalities, rigour and depth of evaluation the ICT product, service or process should undergo;
- An ECCS may specify several evaluation levels depending on rigour and depth of the methodology used, each level corresponding to one of assurance levels and defined by an appropriate combination of assurance components.

The EU Cybersecurity Act stipulates that an ECCS should have the following *elements:* Subject matter and scope, including the type or categories of ICT products, services and processes;

- A clear description of its purpose and how selected standards, evaluation methods and assurance levels correspond to the needs of scheme's intended users;
- References to international, EU or national standards applied in evaluation or, if not appropriate, to technical specifications that meet requirements for ICT specifications set out in Regulation (EU) No. 1025/2012 on EU standards or to technical specifications or other cybersecurity requirements defined in the ECCS;
- One or more assurance levels, as applicable;
- An indication of whether conformity self-assessment (CSA) is permitted under the scheme, and specific or additional requirements to which CABs are subject (where applicable);
- Specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved;
- Where applicable, information necessary for certification (to be supplied or made available to the conformity assessment bodies by an applicant);
- Conditions under which marks or labels that may be used (if the scheme provides for them);
- Rules for monitoring compliance of ICT products, services and processes with requirements of ECCs or ESoCs (including mechanisms to demonstrate continued compliance with them);
- Where applicable, conditions for issuing, maintaining, continuing and renewing ECCs and conditions for extending or reducing the scope of certification;
- Rules on consequences for ICT products, services and processes possessing an ECC or ESoC but which do not comply with scheme's requirements;
- Rules on reporting and dealing with previously undetected cybersecurity vulnerabilities in ICT products, services and processes;
- Where applicable, rules on retention of records by conformity assessment bodies;

- Identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, services and processes, and security requirements, evaluation criteria and methods and assurance levels;
- Content and format of ECCs and ESoCs to be issued;
- Period of availability of the ESoC, technical documentation and all other relevant information to be made available by the manufacturer or provider of ICT products, services or processes;
- The maximum period of validity of ECCs issued under the scheme;
- Disclosure policy for the ECCs issued, amended or withdrawn under the scheme;
- Conditions for the mutual recognition of certification schemes with third countries;
- Where applicable, rules concerning any peer assessment mechanism established by the scheme for national authorities or bodies issuing ECCs for 'high' assurance level; such a mechanism without prejudice to peer review regulated under Article 59;
- Format and procedures to be followed by manufacturers or providers of ICT products, services or processes in supplying and updating supplementary cybersecurity information.

The EU Cybersecurity Act also stipulates that the following ***additional information for certified ICT products, services and processes*** should be made publicly available by the manufacturer or provider:

- Guidance and recommendations to assist end users with secure configuration, installation, deployment, operation and maintenance of ICT products or services;
- The period during which security support will be offered to end users, in particular as regards availability of cybersecurity related updates;
- Contact information of manufacturer or provider and accepted methods to receive vulnerability information from end users and security researchers;
- A reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, service or ICT process and to any relevant cybersecurity advisories.

The *establishment/updating of an EU cybersecurity certification scheme* starts with an EC request to ENISA to prepare a candidate scheme, from the list of ECCSs included in the EU rolling programme (or not part of it, when justified, and the latter is updated accordingly). Then ENISA prepares a candidate scheme that meets requirements set out in the EU Cybersecurity Act (when refusing an EC request, it should provide the reasons, and the final decision is taken by the Management Board). ENISA prepares a candidate scheme through an *ad hoc* working group of experts (including from MSs). It does this in a formal, open, transparent and inclusive consultation process with all relevant stakeholders, and also may take into account a non-binding opinion submitted by ECCG, which also provides ENISA with assistance and expert advice in this process. Finally, the EC may adopt an ECCS for ICT products, services and processes (it may also adopt implementing acts for this purpose) that meet the security objectives, assurance levels and elements outlined above. ENISA

evaluates each adopted ECCS at least every five years, taking into account the feedback received from interested parties.

The EU Cybersecurity Act sets the following rules for ***EU cybersecurity certification*** (ECC): ECC is voluntary, unless otherwise specified by EU or MS law;

- The EC regularly assesses the efficiency and use of the adopted ECCSs (the first one to be done by the end of 2023) and whether a specific one is to be made mandatory through relevant EU law;
- ECC is voluntary, unless otherwise specified by EU or MS law;
- The EC regularly assesses the efficiency and use of the adopted ECCSs (the first one to be done by the end of 2023) and whether a specific one is to be made mandatory through relevant EU law;
- Priority for assessment by the EC – at least latest two years after the adoption of the first ECCS – should be given to ECCs in essential services listed in Annex II of Directive (EU) 2016/1148: energy (electricity, oil and gas), transport (air, rail, water, road), banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructure;
- The EC assessment should take into account the following elements: impact of measures on manufacturers or providers of ICT products, services or processes and on the users in terms of the cost of those measures and societal or economic benefits stemming from anticipated enhanced level of security for them; existence and implementation of relevant MS and third country law; an open, transparent and inclusive consultation process with all relevant stakeholders and MSs; implementation deadlines, transitional measures and periods, particularly regarding the possible impact on manufacturers or providers of ICT products, services or processes, including SMEs; and propose the most speedy and efficient to implement the transition from a voluntary to mandatory certification schemes;
- EU cybersecurity conformity assessment certificates (ECCACs) for ECCSs requiring 'basic' or 'substantial' assurance levels are issued by accredited conformity assessment bodies (CABs), pursuant to Article 60 of the EU Cybersecurity Act; as a derogation from this rule, an ECCAC may, in duly justified cases, be issued only by a public body that is either a national cybersecurity certification authority (NCCA) or accredited as a CBA pursuant to Article 60 of the EU Cybersecurity Act;
- ECCACs for ECCSs requiring a 'high' assurance level are issued only by an NCCA or by a CBA upon prior approval by the NCCA, or on the basis of a general delegation of this task by it;
- The natural or legal person submitting ICT products, services or processes for certification makes available to the NCCA (where it is the body issuing the ECC) or to the CBA all information necessary to conduct the certification;
- The holder of an ECC should inform the issuing NCCA or CBA of any vulnerabilities or irregularities detected subsequently concerning security of the ICT product, service or process that may impact its compliance with certification related

requirements; the latter should forward it, without undue delay, to the NCCA concerned;
- An ECC is issued for the period provided for in the ECCS and may be renewed, provided that the relevant requirements continue to be met;
- An ECC issued pursuant to this Article of the EU Cybersecurity Act must be recognised in all MSs.

The EU Cybersecurity Act also sets the following rules for ***conformity self-assessment*** (CSA):
- An ECCs may allow for the CSA under the sole responsibility of the manufacturer or provider of ICT products, services or processes, and is permitted only in relation to low-risk / 'basic' assurance level ICT products, services and processes;
- The manufacturer or provider of an ICT product, service or process may issue an ESoC stating that the fulfilment of requirements set out in the ECCS has been demonstrated, it thus assumes the responsibility for its compliance with respective requirements;
- The manufacturer or provider in question should make the ESoC, technical documentation, and all other relevant information available to the NCCA for the period provided for in the respective ECCS, and should submit a copy of the ESoC to NCCA and to ENISA;
- The issuance of an ESoC is voluntary, unless otherwise specified in EU or MS law, and is recognized by all MSs.

The EU Cybersecurity Act stipulates that in cases when the EC establishes an ECCS for ICT products, services and processes through an implementing act, ***national cybersecurity certification schemes and certificates*** cease to exist upon its entry into force. Such national schemes that are not covered by an ECCS, and related procedures, remain in place. At the same time, MSs are not allowed to introduce such national schemes ICT products, services and processes already covered by an ECCS that is in force, but such certificates already issued are valid until their expiry date. In order to avoid market fragmentation, MSs are also obliged to inform the EC and ECCG of any intention to draw up new national cybersecurity certification schemes.

The EU Cybersecurity Act also provides for ***peer review*** for NCCAs, aimed at achieving equivalent standards throughout the EU in respect of ECCs and ESoCs. Peer review exercises focus particularly on: whether their ECCs issuance and supervisory activities are strictly separated and carried out independently from each other; procedures for supervising and enforcing rules for monitoring compliance of ICT products, services and processes with ECCs; procedures for monitoring and enforcing obligations of manufacturers or providers of ICT products, services or processes; procedures for monitoring, authorising and supervising activities of CABs; and whether staff of authorities or bodies issuing certificates for 'high' assurance level have the appropriate expertise. They are carried out at least once every five years, based on sound and transparent evaluation criteria and procedures, by at

least two NCCAs and the EC, and ENISA may also participate. As follow-up on outcomes of peer reviews, ECCG draws up summaries and, as needed, issues guidelines or recommendations on actions to be taken by respective NCCAs. The EC may regulate peer reviews through implementing acts, taking into account ECCG's views.

Under the EU Cybersecurity Act NCCAs are also required to ***notify*** the EC on CABs accredited for each ECCS and changes thereto, including, as needed, on CABs with higher expertise, depending on assurance levels. One year after the entry into force of an ECCS the EC publishes the list of accredited CABs in the EU Official Journal and has to publish amendments within two months after receiving respective notifications from NCCAs. The EC may regulate notification through implementing acts as well.

The last three aspects of the procedural chain regulated by the EU Cybersecurity Act are the following: the right to complaint and to judicial remedy and penalties. ***Complaints*** against an issuer of an EU cybersecurity certificate (ECC) or a conformity assessment body (CAB), when applicable, may be lodged by natural and legal persons, in the latter case against the respective NCCA. They also have the right to be informed by the receiver of the complaint on progress of proceedings and on the right to ***judicial remedy***. Natural and legal persons have the right to judicial remedy with regard to decisions of an issuer of an ECC or a CAB, including in relation to improper issuing, failure to issue or recognition of an ECC held by those natural and legal persons; and in response to the latter's failure to act on a complaint. Such cases are adjudicated by courts of the MS in which the authority or body against which the judicial remedy is sought is located. Last but not least, MSs are obliged to lay down rule on ***penalties*** applicable to infringements of provisions of the EU Cybersecurity Act on ECCF and of ECCSs, and to take measures to implement them, as well as to notify the EC on those rules and measures and amendments affecting them.

The ***institutional setup*** foreseen by the EU Cybersecurity Act to manage the EU cybersecurity certification framework (ECCF) consists of three entities: national cybersecurity certification authorities (NCCAs), conformity assessment bodies (CABs) and the European Cybersecurity Certification Group (ECCG).

Each MS has to designate one or more *national cybersecurity certification authorities* in its territory or, with the agreement of another MS, to designate one or more NCCA established in that MS as responsible for supervisory tasks in the designating MS, and to inform the EC. Each NCCA is independent of the entities it supervises in its organisation, funding decisions, legal structure and decision-making. MSs also have to ensure that NCCAs have adequate resources to ensure their effective and efficient functioning and that their ECC issuance and supervisory activities are carried out independently from each other. The EU Cybersecurity Act also promotes active participation of NCCAs in the ECCG. NCCAs' main functions related to ECCF are to:

- Supervise and enforce rules included in ECCSs for monitoring compliance of ICT products, services and processes with requirements of ECCs issued in their respective territories, in cooperation with other relevant market surveillance authorities;
- Monitor compliance with and enforce obligations of manufacturers or providers of ICT products, services or processes operating and carrying out CSAs in their territory, and in particular their compliance with and enforcement of their obligations to issue ESoCs and within respective ECCSs;
- Assist and support national accreditation bodies in monitoring and supervising CABs' activities for the purpose of the EU Cybersecurity Act;
- Where applicable, authorise CABs with specific or additional requirements, and restrict, suspend or withdraw authorisations where CABs infringe requirements of the EU Cybersecurity Act;
- Withdraw, in accordance with national law, ECCs issued by NCCAs or ECC issued by CABs for ICT products, services and processes with the 'high' assurance level in case of non-compliance with the EU Cybersecurity Act or an ECCS;
- Deal with complaints, including by conducting investigations, of natural or legal persons in relation to ECCs issued by NCCAs or ECCs issued by CABs for ICT products, services and processes with the 'high' assurance level or to ESoCs for the 'basic' assurance level;
- Audit CABs, ECC holders and ESoC issuers to verify their compliance with Acts provisions on ECCF, as well as take appropriate measures, in accordance with national law, to ensure their compliance with the EU Cybersecurity Act or ECCSs;
- Impose penalties, in accordance with national law and the EU Cybersecurity Act and require immediate cessation of infringements of obligations set out in the EU Cybersecurity Act;
- Report annually to ENISA and ECCG on their compliance monitoring and supervising activities related to ICT products, services and processes;
- Cooperate with other NCCAs or other public authorities, including by sharing information on possible non-compliance of ICT products, services and processes with requirements of the EU Cybersecurity Act and specific ECCSs, as well as request CABs, ECC holders and ESoC issuers information needed to perform their tasks;
- Cooperate with other NCCAs and the EC, in particular though exchange of information, experience and good practices on cybersecurity certification and related technical issues for ICT products, services and processes;
- Monitor relevant developments in the area of cybersecurity certification.

Each MS, namely their accreditation bodies, is obliged to accredit *conformity assessment bodies* pursuant to the Regulation (EC) No 765/2008 on requirements for accreditation and market surveillance relating to marketing of products. In order to be accredited, CABs must meet requirements set out in the Annex of the EU Cybersecurity Act. In cases when an ECC is issued by an NCCA, the certification body of that NCAA also has to be accredited as CAB,

while if the ECCS has set out specific or additional requirements, only CABs that meet those requirements can be authorised by the NCCA to carry out tasks under such schemes. Accreditation to CABs is issued for a maximum period of five years, with the possibility of being renewed upon meeting the same conditions, accreditation can be restricted, suspended or revoked where conditions have or are no longer met or when a CAB infringes the EU Cybersecurity Act.

The EU Cybersecurity Act establishes the *European Cybersecurity Certification Group* as a collegial body representing MSs', through NCCAs or other relevant authorities, also with the option of one NCCA to representing two MSs. Stakeholders and relevant third parties may also be invited to attend ECCG meetings and to participate in its work. The EC chairs the ECCG and provides it with a secretariat. ECCG has the tasks to:

- Advise and assist the EC in implementation of this Act's provisions on the ECCF, in particular regarding the EU rolling work programme, cybersecurity certification policy issues, coordination of policy approaches and preparation of ECCSs;
- Assist, advise and cooperate with ENISA in preparing a candidate ECCS, by requesting ENISA to prepare it, adopting an opinion on it prepared by ENISA and opinions addressed to the EC relating to existing ECCSs' maintenance and review;
- Examine relevant developments on cybersecurity certification and exchange information and good practices on cybersecurity certification schemes;
- Facilitate cooperation among NCCAs related to ECCF through capacity-building and information exchange;
- Support implementation of peer assessment mechanisms for 'high' assurance level ICT products, services and processes;
- Facilitate alignment of ECCSs with internationally recognised standards, including by reviewing existing ones and recommending ENISA to engage with relevant international standardisation organisations to address insufficiencies or gaps in such standards.

Another mechanism required by the EU Cybersecurity Act is a dedicated official **webpage for the EU cybersecurity certification schemes**. It provides information on ECCSs and ESoCs, and supplementary information on certified ICT products, services and processes. It also indicates national cybersecurity certification schemes replaced by EU ones. It is accessible at https://certification.enisa.europa.eu.

Integration of WB6 Countries into the European Union Cybersecurity Agency: State of Play

This section discusses the area of cybersecurity in each WB6 country. It does so by focusing on two aspects. One is the state of play with regard to legislation, policies and institutional framework. The other aspect are key reform priorities in their ongoing reform processes carried out in the context of these countries' EU accession processes.

Looking at the most recent EC's annual reports assessing the state of play of EU integration reforms in each WB6 country, published in November 2023, the area of cybersecurity is discussed in all of them. However, none contains any reference to ENISA specifically or integration into it. These reports also identify key challenges for each country and recommend priority short-term reforms to implement in this area for alignment with and implementation of EU legislation and standards. Concerning the legal framework, they also refer to the 2001 Council of Europe (CoE) Budapest Convention on Cybercrime[33], of which all WB6 countries but Kosovo are signatory parties to. Overall, all WB6 countries have put in place a framework (legally, policy-wise and institutionally) in the area of cybersecurity, or are working towards this goal. They can therefore be considered to have basic preconditions to also formally start engaging in the reform process for integration into ENISA.

In the context of this forward looking reform process it is important to underline that the EU has included integration of the Western Balkans region into the EU Digital Single Market (DSM) as one of the seven strategic priority areas in the Reform and Growth Facility for the Western Balkans (RGF)[34] launched in November 2023. This means that cybersecurity will be one of specific policy areas that will be tackled with high priority across the region in terms of both reforms and financial investments to further advance towards EU standards in this area. As a highly ambitious reform initiative coming from the EU for the entire region for the next medium-term period, until 2027/2028 – also containing the same policy areas and reforms for all countries and a very significant financial package of €6 billion – RGF is a huge boost in terms of reform incentives and financial resources to invest. As such, it is expected to significantly improve WB6 countries' preparedness for EU membership and economic convergence within the region and with the EU market, including the digital market.

Albania has adopted its amended Cybersecurity Law in 2024[35] and 2020-2025 Cybersecurity Strategy.[36] It is also party to the Budapest Convention and the Second

[33] *Council of Europe, The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols, https://www.coe.int/en/web/cybercrime/the-budapest-convention.*

[34] *European Commission, New Growth Plan for the Western Balkans, https://neighbourhood-enlargement.ec.europa.eu/enlargement-policy/new-growth-plan-western-balkans_en#the-structure-of-the-growth-plan.*

[35] *National Cybersecurity Authority of Albania, Law on Cybersecurity (in Albanian), https://aksk.gov.al/wp-content/uploads/2024/04/ligj-2024-03-21-25-5.pdf.*

[36] *National Cybersecurity Authority of Albania, National Cybersecurity Strategy and its Action Plan 2020-2025, https://aksk.gov.al/wp-content/uploads/2023/06/National-Cybersecurity-Strategy-and-its-Action-Plan-2020-2025.pdf.*

Additional Protocol on enhanced co-operation and disclosure of electronic evidence. Albania has its institution in charge of cybersecurity (the National Cybersecurity Authority), a National Cybersecurity Coordinator and the National Authority on Electronic Certification and Cybersecurity. In response to the 2022 cyberattacks, it has created a government cybersecurity operations centre (in charge of cybersecurity incidents and crises within governmental systems), increased the list of critical information infrastructures from 140 to 289 (now covering sectors of government, energy, health, finance, transport, digital and water supply). It has also strengthened cybersecurity capacities (through training on cybercrime prevention indicators) and increased the number of cybercrime and internet fraud cases by 65% in 2022. On international cooperation, in 2022 Albania participated in 119 actions against organized crime and cyberattacks, strengthened cooperation with Italy in fighting cybercrime, and has concluded cybersecurity agreements with Israel, Saudi Arabia and United Arab Emirates.[37]

On further reforms, the EC has identified two *key short-term priorities*: (1) Adopting relevant legislation to enact the cybersecurity law, with a view to ensuring closer alignment with the EU directive on measures for a high common level of cybersecurity across the Union (NIS II); and (2) Achieving more results in countering cybercrime (in particular prosecution). Other priorities include adoption of the new legislation foreseen in the new Cybersecurity Strategy, countering cybercrime (focusing on detection, traceability and prosecution), capacity-building and awareness raising, strengthening digital security and protection of personal data, and strengthening cooperation with the private sector and civil society.[38]

Bosnia and Herzegovina is party to the Budapest Convention, but it only implements it partially and has yet to sign the Second Additional Protocol and it has no national cybersecurity agency in place. On further reforms, the EC has identified one *key short-term priority*: Developing a legislative framework on cybersecurity in line with the acquis. Other priorities include adoption of a cybersecurity law (for further alignment with the acquis) and strategy, establishing a single point of contact and a CSIRT network, fighting cybercrime and capacity-building to do so, strengthening law enforcement cooperation, as well as addressing vulnerability to cyberattacks and hybrid threats (through an overall assessment and a policy framework).[39]

Kosovo has adopted its Cybersecurity Law in 2010 and amendments to it in 2023 (partially aligned with the NIS Directive), as well as the 2023-2027 Cybersecurity Strategy, but is not

[37] *European Commission, Albania 2023 Report, pp. 17, 34, 43-44, 77, 83, 95, https://neighbourhood-enlargement.ec.europa.eu/document/download/ea0a4b05-683f-4b9c-b7ff-46154fffd0b_en?filename=SWD_2023_690%20Albania%20report.pdf.*

[38] *Ibid, pp. 4-5, 17, 41, 43, 46, 94-95.*

[39] *European Commission, Bosnia and Herzegovina 2023 Report, pp. 43, 49, 52, 97-98, 131, https://neighbourhood-enlargement.ec.europa.eu/document/download/e3045ec9-f2fc-45c8-a97f-58a2d9b9945a_en?filename=SWD_2023_691%20Bosnia%20and%20Herzegovina%20report.pdf.*

yet a signatory party to the Budapest Convention. On the institutional setup, it has established its dedicated Cybersecurity Agency in 2022 and cybercrime directorate in Kosovo Police, and in general has basic cybersecurity capabilities. On law enforcement, the number of cybercrime cases has increased by nearly 50% from 2021 to 2022. On further reforms, the EC has identified two *key short-term priorities*: (1) Concluding alignment of the legislation with the EU NIS II Directive and the 5G Cybersecurity Toolbox; and (2) Increasing resources. On other priorities, Kosovo needs to further strengthen operational mechanisms, technical capacities and human resources to fight cybercrime, including through more training for newly appointed judges and prosecutors and those handling electronic evidence.[40]

Montenegro also has its Cybersecurity Law and the Cybersecurity Strategy in force, and is a signatory party to the Budapest Convention and the Second Protocol.[41] On the institutional setup, Montenegro has made preparations to establish the cybersecurity agency[42], while it has established the government CIRT (the new Directorate on Information Security within the Ministry of Public Administration). On law enforcement, it has substantially increased its capacity to fight cybercrime and increased the number of investigations for cyber related offences, but there was no final court decision. On further reforms, Montenegro needs to align its legislation with the 5G Cybersecurity Toolbox, e-Privacy Directive and the eIDAS Regulation on digital identity and trust services, as well as to strengthen institutional capacities. On law enforcement, it needs to ensure effective, proportionate and dissuasive penalties in cybercrime cases, while reporting of cybercrime and cyber incidents need to increase through public awareness raising on risks and threats. Assessment of cyber and hybrid threats also needs to be improved.[43]

North Macedonia does not yet have a cybersecurity law in force and its cybersecurity has expired at the end of 2022 and the new one has yet to be adopted. It is a signatory party to the Budapest Convention and has signed its Second Protocol. On the institutional setup, it does not yet have a cybersecurity agency, but has established a National Cybersecurity Council (as a coordination body consisting of ministers of interior, defence and information society and public administration) and the national CIRT (the latter promotes cybersecurity through response to cyber incidents). The Ministry of Interior's Computer Crime and Digital Forensics Sector carries out investigations into cybercrime and the army is developing cyber

[40] *European Commission, Kosovo 2023 Report, pp. 43-45, 48, 95-96, https://neighbourhood-enlargement.ec.europa.eu/document/download/760aacca-4e88-4667-8792-3ed08cdd65c3_en?filename=SWD_2023_692%20Kosovo%20report_0.pdf.*

[41] *Ibid, pg. 59.*

[42] *Government of Montenegro, Crna Gora dobija Agenciju za sajber bezbjednost, https://www.gov.me/clanak/crna-gora-dobija-agenciju-za-sajber-bezbjednost.*

[43] *European Commission, Montenegro 2023 Report, pp. 52, 59, 62, 102, https://neighbourhood-enlargement.ec.europa.eu/document/download/e09b27af-427a-440b-a47a-ed5254aec169_en?filename=SWD_2023_694%20Montenegro%20report.pdf.*

defence capacities and cooperates with international organisations in the field of global cyber security and hybrid threats. On law enforcement, 287 cybercrime criminal acts were registered in 2022 and cyber-related incidents were reported in 145 entities. On further reforms, the EC has identified one *key short-term priority*: to adopt the 2023-2027 national cybersecurity strategy. On other priorities, it needs to improve coordination and inter-institutional cooperation, as well as to further strengthen cyber capacities and infrastructure.[44]

Serbia has its Information Security Law in force and is a signatory party to the Budapest Convention and its Second Protocol, while its cybersecurity strategy has expired at the end of 2023. On the institutional setup, it has not yet established a cybersecurity agency, but has established its national CERT and a Special Prosecutor's Office for Cybercrime. On further reforms, Serbia needs to continue aligning its legislation with the EU acquis, including with the NIS II Directive, as well as to strengthen and upgrade its institutional capacities, including for investigation of cybercrime, cyber incidents and other forms of abuse on the internet.[45]

Integration of WB6 Countries into the European Union Cybersecurity Agency: A Proposed Roadmap

Based on the analysis of the ENISA Regulation and of the state of play of each WB6 country in the area of cybersecurity, this paper proposes main reform activities for their phased integration into ENISA. These reforms are of two types: substantial reforms and process oriented ones.

[44] *European Commission, North Macedonia 2023 Report, pp. 41, 89-90, https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_693%20North%20Macedonia%20report.pdf.*
[45] *European Commission, Serbia 2023 Report, pp. 59-60, 112, https://neighbourhood-enlargement.ec.europa.eu/document/download/9198cd1a-c8c9-4973-90ac-b6ba6bd72b53_en?filename=SWD_2023_695_Serbia.pdf.*

What reforms need to be prioritised by WB6 for gradual integration into ENISA?

The following main *substantial* reform priorities for WB6 countries' phased integration into ENISA need to be pursued:

No	Priority	State of Play
1.	Each WB6 country is required to have its national cybersecurity law in force and implementing it.	• Albania has the Law No. 25/2024 on Cybersecurity in force; • Bosnia and Herzegovina does not yet have a national-level cybersecurity law in force; • Kosovo has the Law No. 08/L-173 on Cybersecurity in force; • North Macedonia does not yet have a national-level cybersecurity law in force; • Serbia does not yet have a national-level cybersecurity law in force.
2.	Each WB6 country is required to align its national cybersecurity law and implementing legislation with provisions of acquis acts in the area of cybersecurity that are relevant for membership into ENISA, in particular with the following acts	• Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act); • 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; • Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast); • Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; • Regulation (EC) No. 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No. 339/93;

		• Regulation (EC) No. 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council; • Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); • Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); • Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.
3.	Each WB6 country is required to have its valid national cybersecurity strategy adopted and being implemented	• Albania has adopted the National Cybersecurity Strategy and Action Plan 2020-2025; • Bosnia and Herzegovina has not yet adopted a national-level cybersecurity strategy; • Kosovo has adopted the National Cyber Security Strategy 2023-2027; • North Macedonia does not have a valid national-level cybersecurity strategy; • Serbia does not have a valid national-level cybersecurity strategy.
4.	Each WB6 country is required to have its national cybersecurity agency established and functional	• Albania has established its national cybersecurity agency – National Cyber Security Authority (NCSA); • Bosnia and Herzegovina has not yet established its national cybersecurity agency; • Kosovo has established its national Cybersecurity Agency;

		• North Macedonia has not yet established its national cybersecurity agency; • Serbia has not yet established its national cybersecurity agency
5.	Each WB6 country is required to have its Cybersecurity Emergency Response Team (CERT) / Computer Security Incident Response Team (CSIRT) established and functional	
6.	Each WB6 country needs to develop and implement its national cybersecurity certification framework (NCCF) for ICT products, services and processes, in line with the EU Cybersecurity Act and EU standards and best practice. Such a framework needs to have the following components	• National programme for cybersecurity certification, as a medium-term planning tool to implement the NCCF; • Security objectives of its national cybersecurity certification schemes; • National cybersecurity certification schemes with its elements; • Assurance levels of its national cybersecurity certification schemes: basic, substantial and high; • Conformity assessment and self-assessment; • Cybersecurity certification, including the authorities in charge; • Supplementary security information for certified ICT products, services and processes; • Conformity assessment and conformity assessment bodies; • Peer review; • Notification • Right to complain and to judicial remedy, and penalties; and • Official webpage of the NCCF.
7.	As required by the EU Directive on security of network and information systems across the Union, each WB6 country needs to address with priority essential services, by designing the list of such services and treating them in line with EU cybersecurity acquis, standards and best practices. In order to ensure effective compliance and enforcement, it is adequate that such a list is provided for under a dedicated legal provision of the national cybersecurity law and further detailed in an annex. As discussed above, such a list in the EU includes services in areas of energy, transport, banking, financial market infrastructures, health, drinking water and digital infrastructure.	

What options are available for gradual integration in ENISA of the WB6?

The European Commission – in cooperation with ENISA and its decision-making bodies, Member States and each WB6 country – needs to conduct formal dialogues/negotiations on their membership to / cooperation with ENISA, and make a political decision on this. There are two options to achieve this: membership or cooperation with third countries.

Membership of WB6 countries through phased integration from observer members to full members, in parallel with meeting requirements and standards at the same level as EU Member States. This is the most favourable option for WB6 countries, and as such advocated by this policy brief. However, in also requires political will and consensus among member states. Provided there is political will and consensus on the part of the EU, during the transition until WB6 countries become EU member states they could be granted the legal status of observer members and become full members upon their formal accession to the EU. However, currently there is no legal basis for this because the EU Cybersecurity Act does not provide for any form of membership for countries other than EU Member States. Therefore, establishing the legal basis for phased integration of WB6 countries, as EU accession countries, from observers to full members would require amending the EU Cybersecurity Act in order to add provisions providing for this and provisions setting out their rights and obligations.

Cooperation with WB6 countries as third countries until their full membership of ENISA once they become EU Member States. This option is less favourable for these countries, but it is one for which there is already a legal basis in the EU Cybersecurity Act (Art 12 and 42). This option could be implemented through bilateral international agreements with each WB6 country individually, which would be signed/concluded between the EC and WB6 countries' Governments, and ratified by the EU and each WB6 country as foreseen by respective constitutional and legal provisions governing international agreements. While this option is less time consuming to implement – because it does not require amending the EU Cybersecurity Act – it is less attractive for WB6 countries in terms of EU accession driven reform incentives in the area of cybersecurity.

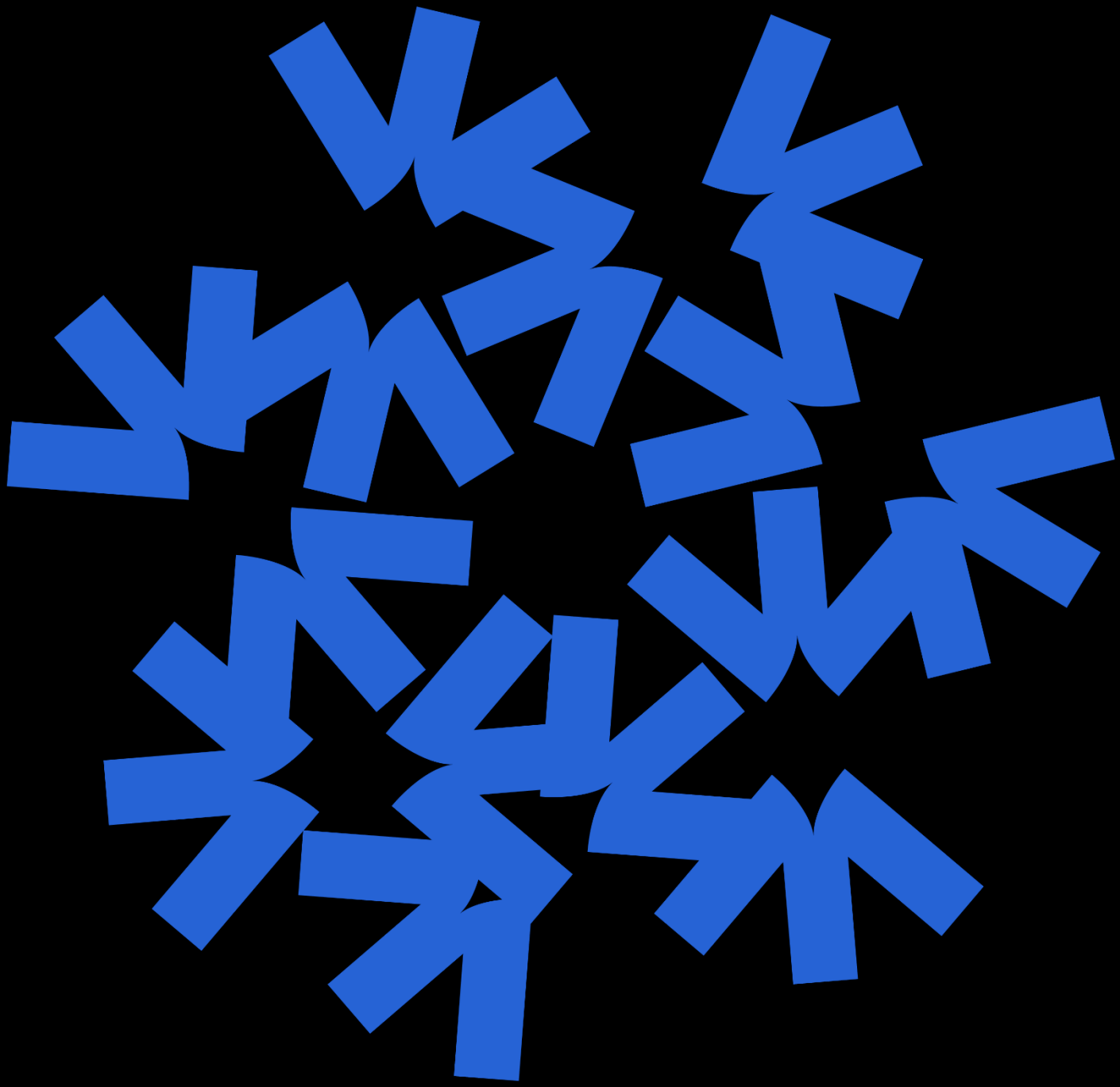
Once such a decision is made by the EU, the Government of each WB6 country need to formally appoint the head of its national cybersecurity agency as a National Liaison Officer. They need to be in charge of formal relations with ENISA both prior and after membership in / cooperation with ENISA is formally established.

What WB6 countries need to do for gradual integration in ENISA?

Process-wise, the following main reform activities for WB6 countries' phased integration into ENISA need to be pursued:

8. Each WB6 country and the EU (through the EC, in cooperation with ENISA) need to carry out feasibility studies on the state of play in each WB6 country on phased integration into ENISA, scanning the state of play and identifying reforms for both sides towards this end.
9. All WB6 countries need to update their national cybersecurity laws and other legal acts to address gaps identified in the feasibility studies, with a view to achieving a level of compliance with the ENISA Regulation and other relevant acquis that is satisfactory for integration into ENISA.
10. All WB6 countries need to update their national cybersecurity strategies to address gaps identified in the studies, with a view to put in place policies to implement and enforce the acquis-compliant legislation towards integration into ENISA.
11. Based on the ENISA Regulation and feasibility studies on WB6 countries' phased integration into ENISA, the EC (in cooperation with ENISA) needs to prepare and publish a single list of preconditions and criteria for WB6 countries' integration into ENISA.
12. Based on its national cybersecurity law and strategy, as well as on the ENISA Regulation and other applicable legislation and the feasibility study on its phased integration into ENISA, each WB6 country (in consultation with the EC and ENISA) needs to prepare, adopt and implement its roadmap for phased integration into ENISA.
13. Each WB6 country (through its Government) and the EU (through the EC and ENISA) need to set up joint institutional structures to coordinate and oversee the reform dialogue for its phased integration into ENISA.

The European Commission needs to start assessing the progress of each WB6 country in its phased integration into ENISA in its annual Country Reports assessing its EU accession progress.



KCSS
Kosovar Centre for Security Studies

Ignita
Igniting Collaboration

OPEN SOCIETY
FOUNDATIONS
WESTERN BALKANS