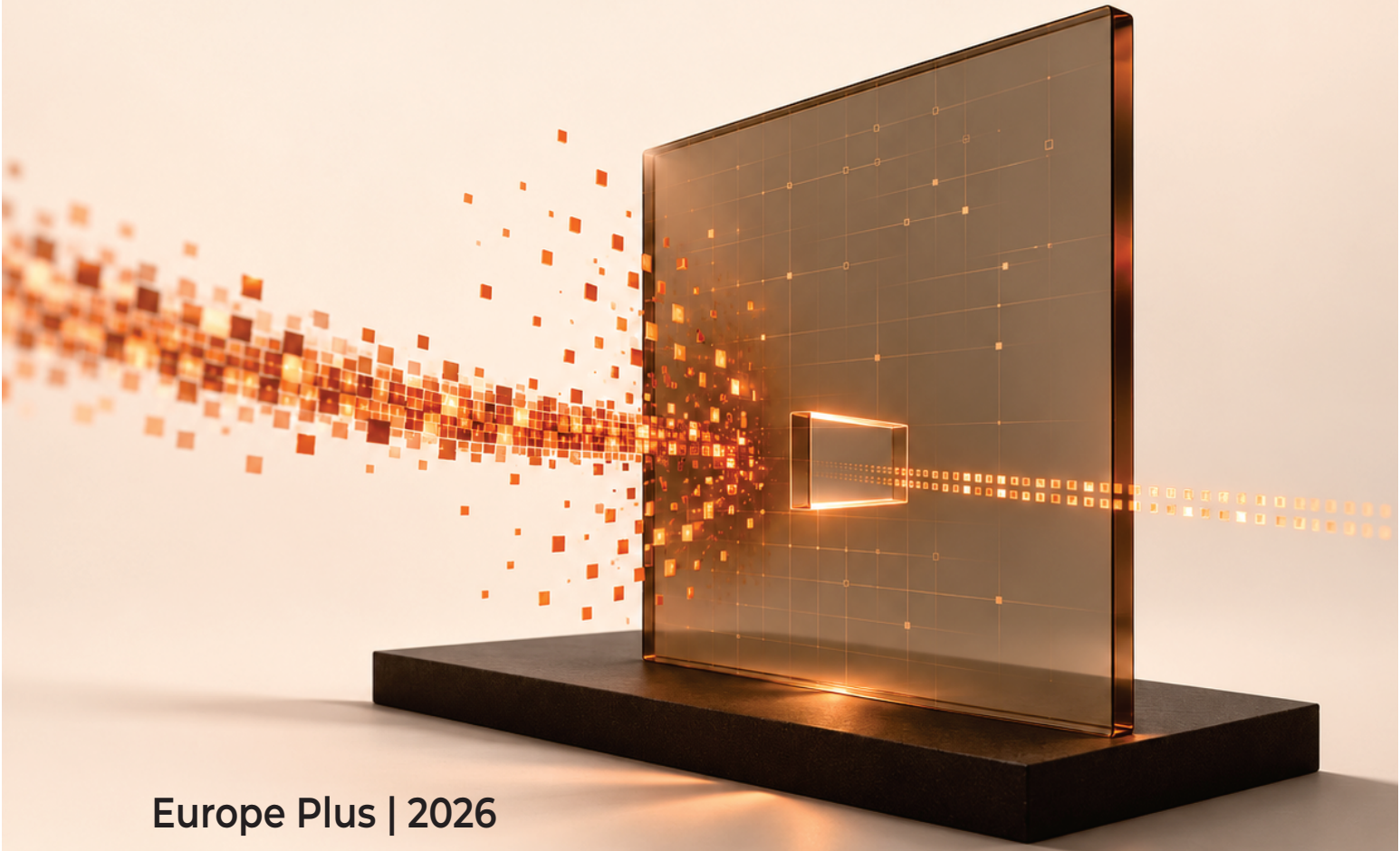
Cybersecurity & Regional Resilience

Policy, Governance and Coordination in the Western Balkans



Europe Plus | 2026



CYBERSECURITY & REGIONAL RESILIENCE

Policy, Governance and Coordination in the Western Balkans

Disclaimer

This publication was produced by Europe Plus within the framework of the Regional Executive Programme for Cooperation and Transformation (REPACT).

The contents of this publication are the sole responsibility of Europe Plus and do not necessarily reflect the views, opinions, or positions of the project's donors, partners, or any other institution or organisation supporting or cooperating in the implementation of the project.

This publication is an intellectual product developed for research, policy analysis, capacity-building, and advocacy purposes.

Copyright © 2026 Europe Plus. All rights reserved.

Brief extracts from this publication may be quoted or reproduced for non-commercial purposes, including research, education, and policy analysis, provided that full acknowledgement is given to Europe Plus as the source. No part of this publication may be reproduced, republished, translated, adapted, distributed, stored in a retrieval system, or transmitted in any form or by any means, in whole or in part, for commercial purposes or without prior written permission from Europe Plus.

CONTENTS

1. Background and Rationale 5
2. Module Objective 6
3. Target Audience 6
4. Duration and Delivery Format 7
5. Learning Outcomes 7
6. Module Structure and Thematic Areas 7
7. Training Methodology 13
8. Cross-Cutting Integration 14
9. Expected Impact 14
ANNEX I 14
Background Material
Cybersecurity, Digital Integration and Regional Cooperation
in the Western Balkans
1. Cybersecurity as a Governance Issue 14
2. Cyber Risks in an Increasingly Inter-connected Region 15
3. Cybersecurity and the Common Regional Market 16
4. EU Frameworks and the Changing Nature of Integration 17
5. The Growth Plan and Gradual Integration in the Digital Domain 18
6. Digital Trust, Data Protection and Institutional Accountability 19
7. The Need for Regional Coordination 19
8. From Risk Management to Resilience 20



ANNEX II: Key References 20

PART I 21
EU Cybersecurity Legislative Framework
Directive (EU) 2022/2555 (NIS2 Directive)

PART II 23
EU Digital Policy Framework
EU Cybersecurity Strategy for the Digital Decade (2020)

PART III 24
Enlargement and Regional Integration
EU Growth Plan for the Western Balkans

PART IV 25
European Cybersecurity Governance

PART V 26
Recommended Case Studies

PART VI 27
Suggested Pre-Course Reading



1. Background and Rationale

Within the framework of the REPACT – Regional Executive Programme for Cooperation and Transformation, this module addresses the growing importance of cybersecurity and resilience as core policy priorities in the Western Balkans, particularly in the context of EU integration and the implementation of the Common Regional Market (CRM).

As digital systems increasingly underpin public administration, economic activity, and cross-border cooperation, cyber risks are no longer confined to technical domains. They directly affect:

- the continuity and reliability of public services;
- institutional credibility and citizen trust;
- the functioning of markets and economic exchanges;
- regional integration and cross-border systems;
- the resilience of democratic institutions and critical sectors.

Recent cyber incidents affecting public institutions across the region, together with the growing prevalence of hybrid threats and malicious cyber activities targeting both public and private actors, have demonstrated that cybersecurity has become a strategic governance challenge. Addressing these risks requires effective institutional coordination, clear roles and responsibilities, and the capacity to prevent, respond to and recover from disruptive events.

At the same time, recent EU policy developments, most notably the EU Growth Plan for the Western Balkans, have introduced a more operational approach to enlargement, centred on gradual integration into the EU Single Market. Within this framework, the digital domain has emerged as one of the most advanced and tangible entry points for early integration, including through areas such as digital services, electronic identification, payment systems and regulatory alignment with EU standards.



In this context, secure and trustworthy digital systems are no longer only a matter of protection but a precondition for participation in emerging forms of gradual access to the EU market. Cybersecurity and resilience therefore become enabling factors for both the effective functioning of the CRM and the credibility of gradual integration pathways. This shift also reflects a broader evolution in the enlargement process, where progress increasingly depends not only on legislative approximation but also on the institutional readiness required to implement, coordinate and sustain participation in European frameworks and networks.

For the Western Balkans, where regional cooperation and progressive integration into the EU Single Market remain strategic priorities, cybersecurity increasingly emerges as a matter of policy, governance and coordination, requiring whole-of-government and whole-of-society approaches rather than purely technical solutions. This module responds to that need by offering a policy-oriented and practice-driven executive training programme tailored to non-technical stakeholders. It aims to strengthen participants' understanding of cybersecurity as a governance issue, enhance their ability to navigate relevant EU and regional frameworks, and support the development of institutional and regional capacities necessary to advance resilience in an increasingly interconnected digital environment.



2. Module Objective

The objective of this module is to strengthen participants' capacity to understand, assess and address cybersecurity risks as a governance and public policy challenge within the broader context of EU integration and regional cooperation. The module is specifically designed for professionals involved in the coordination, implementation and monitoring of reforms related to the Common Regional Market (CRM) and the EU accession process, rather than technical cybersecurity practitioners.

In particular, the module aims to:

- clarify institutional roles and responsibilities in cybersecurity governance;
- enhance strategic decision-making and interinstitutional coordination in crisis and incident-response situations;
- strengthen understanding of the implications of cybersecurity for the implementation of the Common Regional Market and gradual integration into the EU Single Market;
- address the cross-border nature of cyber risks through regional cooperation and coordinated responses;
- support alignment with relevant EU cybersecurity and digital policy frameworks;
- equip participants with the knowledge required to integrate cybersecurity considerations into broader policy reforms and implementation processes related to EU integration;
- enable informed participation in processes of gradual integration into the EU Digital Single Market, where secure and trustworthy digital systems constitute a key precondition.

3. Target Audience

This module is designed for non-technical professionals, including:

- policymakers and public officials
- representatives of public administration
- CRM coordinators and sectoral regulators
- EU integration practitioners and coordinators involved in the implementation and monitoring of accession-related reforms
- civil society organizations
- business representatives and associations

4. Duration and Delivery Format

- Duration: 3 days (20-24 hours)
- Format: In-person, adaptable to blended/ online

5. Learning Outcomes

By the end of the module, participants will be able to:

- articulate cybersecurity as a governance and public policy issue, and position it within broader processes of digital transformation and EU integration
- identify, and understand cyber risks affecting public services, institutional functioning and economic activity
- understand the interlinkages between cybersecurity, digital trust, data protection and rule of law, and their implications for institutional credibility
- understand the relevance of key EU cybersecurity and digital policy frameworks for the Western Balkans, including their practical implications for alignment
- assess the cross-border dimension of cyber risks and evaluate coordination needs in the context of regional cooperation and the Common Regional Market
- apply structured decision-making approaches in a simulated cyber incident, including role allocation, coordination and communication
- formulate concrete, policy-oriented measures to strengthen institutional preparedness, crisis response and regional resilience
- link cybersecurity preparedness to opportunities and requirements for gradual integration into the EU Digital Single Market.



6. Module Structure and Thematic Areas

The module is structured around a logical learning flow moving from understanding risks → governance responses → coordination → resilience-building. The proposed sessions' structure is indicative and can be adapted based on the available time, specific training objectives and the background of participants. Therefore, sessions may be delivered as standalone units or combined, where appropriate, to ensure coherence, depth of discussion and effective use of training time. This flexibility allows the module to be tailored to different audience profiles and

delivery formats while maintaining its overall learning objectives.

6.1. Session on Cybersecurity as a Governance and Policy Challenge

Objective

To introduce cybersecurity as a strategic governance and public policy issue, highlighting its implications for institutional effectiveness, public trust, economic resilience and the broader processes of digital transformation, regional cooperation and EU integration.



Key Themes

- Moving beyond the technical dimension: why cybersecurity matters for policymakers, public administrators and professionals involved in EU integration and CRM implementation;
- Understanding cyber risks as systemic risks with implications for the functioning and resilience of public institutions;
- The impact of cybersecurity incidents on public service delivery, economic activity, critical sectors and citizens' trust in institutions;
- Cybersecurity as an enabling condition for digital transformation, cross-border cooperation and participation in the EU Digital Single Market;
- The growing importance of institutional coordination, clear governance arrangements and whole-of-government approaches in addressing cyber challenges;
- The role of cybersecurity and resilience within the evolving EU enlargement agenda and gradual integration processes.

Expected Learning Outcome

By the end of this session, participants will be able to understand cybersecurity as a governance and public policy challenge rather than solely a technical issue, recognize its implications for institutional performance and regional integration, and identify why effective coordination and resilience are increasingly important within the context of CRM implementation and the EU accession process.

6.2. Session on Cyber Risks and Their Impact on Governance and Economy

Objective

To enhance participants' understanding of the evolving cyber threat landscape and analyze how cyber risks can affect institutional performance, the continuity of public services, economic activity and broader societal resilience.

Key Themes

- Understanding the contemporary cyber threat landscape and the increasing interconnectedness of digital systems;
- Types of cyber risks affecting public and private actors, including ransomware attacks, data breaches, phishing

campaigns, denial-of-service attacks and disruptions to critical services;

- The exposure of public administration, essential services and critical sectors to cyber threats and their implications for operational continuity;
- The impact of cyber incidents on businesses, market functioning, digital transactions and citizens' confidence in digital systems;
- Institutional vulnerabilities, risk exposure and the cascading effects that cyber incidents can generate across interconnected systems;
- The importance of risk awareness and preparedness as foundations for effective governance and resilience-building.

Practical Component

Participants will undertake a structured group exercise to identify and assess cyber risks related to a selected public service, critical sector or institutional function. Through a simplified risk-mapping approach, they will analyse potential threat scenarios, identify key vulnerabilities and discuss the possible institutional, economic and societal impacts of a cyber incident.

Expected Learning Outcome

By the end of this session, participants will be able to identify and categorise different types of cyber risks, recognise vulnerabilities within their institutional or sectoral contexts, and assess the potential implications of cyber incidents for governance, public service delivery and economic activity.

6.3 Session on EU Cybersecurity Frameworks and Implications for the Western Balkans

Objective

To familiarise participants with the evolving EU cybersecurity and digital policy architecture and examine its implications for institutional readiness, regulatory alignment and the gradual integration of Western Balkan countries into relevant EU frameworks and the Digital Single Market.



Key Themes

- The evolving EU approach to cybersecurity and digital resilience within the broader context of the Digital Decade and the EU Security Union;
- Overview of key EU cybersecurity and digital policy instruments relevant for candidate countries, including:
  - the Network and Information Security Directive (NIS2);
  - the Cyber Resilience Act;
  - the Cyber Solidarity Act;
  - relevant elements of the Digital Identity Framework and other emerging digital initiatives;
- Institutional roles, governance arrangements and responsibilities envisaged under EU cybersecurity frameworks;
- Implications for candidate countries in terms of legislative approximation,

institutional adaptation, coordination mechanisms and capacity development;

- Cybersecurity as an enabling condition for trust, interoperability and participation in cross-border digital services and systems;
- Linkages between cybersecurity governance, the Common Regional Market, the EU Digital Single Market and the broader enlargement agenda;
- Moving beyond compliance: understanding institutional readiness as a prerequisite for meaningful participation in European digital and cybersecurity ecosystems.



Expected Learning Outcome

By the end of this session, participants will be able to interpret the objectives and governance implications of key EU cybersecurity frameworks, assess their relevance for national institutions, and understand the institutional and policy adjustments required to support alignment and gradual integration into EU digital and cybersecurity frameworks.

6.4. Session on Digital Trust, Data Protection and Institutional Responsibility

Objective

To explore the interconnections between cybersecurity, digital trust, data protection and institutional accountability, and assess their implications for effective governance, public confidence and the development of secure and trustworthy digital ecosystems.

Key Themes

- Digital trust as a prerequisite for the adoption of digital public services, the functioning of digital markets and the advancement of cross-border cooperation;
- The relationship between cybersecurity, data protection and the protection of individual rights in increasingly digitalised societies;
- Institutional responsibilities for safeguarding personal and sensitive data, including the importance of clear governance arrangements and organisational cultures of responsibility;
- Transparency, accountability and effective communication in the prevention and management of cyber incidents;
- The role of trust in enabling participation in emerging forms of regional and European digital integration, including interoperable and cross-border digital services;
- Rule of Law considerations in digital environments, including oversight mechanisms, accountability structures and the protection of fundamental rights;
- Balancing security objectives with principles of proportionality, privacy and democratic governance.

Expected Learning Outcome

By the end of this session, participants will be able to analyse the governance dimensions of digital trust and institutional accountability,

assess the interplay between cybersecurity and data protection, and understand how these factors shape public confidence, the credibility of institutions and the successful implementation of digital transformation and integration processes.

6.5. Session on Cybersecurity, Regional Cooperation and Crisis Response in the Context of the Common Regional Market (CRM)

Objective

To explore the regional dimension of cybersecurity risks within the framework of the Common Regional Market (CRM) and strengthen participants' ability to navigate policy-level coordination and decision-making during cyber incidents with cross-border implications.

Key Themes

- The growing interdependence of digital systems underpinning regional cooperation, economic integration and public service delivery in the Western Balkans;
- Cybersecurity risks affecting cross-border digital services and emerging areas of regional integration;
- The potential for cyber incidents to generate cascading effects across economies, institutions and critical sectors beyond national borders;
- Implications of cyber disruptions for regional trade, mobility, digital transactions and trust in shared systems and services;
- Institutional roles, coordination requirements and multi-level governance arrangements in responding to incidents with regional dimensions;
- The importance of information-sharing, communication and cooperation mechanisms in strengthening regional resilience.

Practical Component: Scenario-Based Simu-lation Exercise

Participants will engage in a structured simulation involving a cyber incident affecting a major national digital platform with implications for cross-border economic activities, public services and regional cooperation mechanisms linked to the Common Regional Market.



Working in groups and assuming different institutional roles, participants will be required to:

- assess the nature, scale and potential evolution of the incident;
- identify institutional mandates, leadership structures and decision-making responsibilities;
- establish coordination mechanisms among relevant national actors;
- determine when and how regional cooperation mechanisms should be activated;
- develop a policy-level response strategy balancing operational needs, public confidence and continuity of essential services;

- design communication approaches, including public messaging and stakeholder engagement;
- analyse the implications of the incident for regional cooperation, economic exchanges and the functioning of cross-border systems.

Expected Outputs

- A coordinated incident response and governance framework;
- A clear mapping of institutional roles, responsibilities and reporting lines;
- A communication and stakeholder engagement strategy;
- Recommendations for strengthening regional cooperation and preparedness within the context of the Common Regional Market.



Expected Learning Outcome

By the end of this session, participants will be able to assess the regional implications of cyber incidents, understand the governance and coordination requirements necessary to manage crises with cross-border effects, and apply structured policy-level decision-making approaches to strengthen resilience within the Common Regional Market framework.

6.6. Session on Building Regional Resilience

Objective

To examine how institutions and regional cooperation mechanisms can strengthen resilience to cyber risks by moving beyond reactive approaches towards proactive preparedness, coordinated governance and long-term capacity development.

Key Themes

- Understanding resilience as the ability of institutions and systems to anticipate, withstand, adapt to and recover from disruptive cyber events;
- Preparedness planning and risk-informed decision-making as foundations for effective cybersecurity governance;
- Institutional coordination mechanisms, leadership arrangements and whole-of-government approaches to resilience-building;
- The role of business continuity planning, contingency measures and regular pre-paredness exercises in enhancing institutional readiness;
- Public-private cooperation as an essential component of resilience, recognising the role of private actors in managing critical digital infrastructure and services;
- Regional cooperation frameworks, information-sharing practices and trust-building measures that can strengthen collective resilience in the Western Balkans;
- Learning from past incidents and translating lessons identified into institutional reforms, policy improvements and enhanced preparedness.

Reflection Exercise

Participants will identify priority actions that their institutions and the region could undertake to strengthen cyber resilience, improve coordination mechanisms and enhance preparedness in support of regional cooperation and EU integration objectives.

Expected Learning Outcome

By the end of this session, participants will be able to understand resilience as a governance objective, assess the institutional and regional factors that contribute to preparedness and adaptive capacity, and identify practical measures to strengthen coordination, cooperation and long-term resilience within the context of regional integration and digital transformation.

7. Training Methodology

The module adopts a policy-oriented, participatory and practice-driven learning approach, tailored to the needs of professionals involved in the coordination and implementation of reforms related to the Common Regional Market (CRM) and the EU integration process. The methodology is designed to ensure that participants not only understand key concepts and policy frameworks but are also able to apply them within real-world governance, coordination and decision-making contexts.

The training methodology combines:

- Expert-led inputs and policy briefings, providing participants with a structured overview of key concepts, emerging trends, EU policy developments and their implications for the Western Balkans;
- Facilitated discussions and peer exchange, enabling participants to reflect on national experiences, institutional practices and regional dynamics, while encouraging cross-country learning and the sharing of perspectives;
- Group-based exercises and case discussions, supporting the practical application of concepts to concrete institutional, sectoral and regional contexts, and fostering collaborative problem-solving skills;
- Scenario-based simulation exercises, allowing participants to engage in structured, policy-level decision-making within a realistic crisis environment requiring coordination across institutions and jurisdictions;
- Reflection and action-planning activities, encouraging participants to identify lessons relevant to their institutional responsibilities and consider practical measures to strengthen preparedness, coordination and resilience within their respective contexts.

The methodology emphasises active participation, experiential learning and the exchange of practical experiences, recognising that effective cybersecurity governance and regional resilience depend not only on technical expertise but also on leadership, coordination and informed policy choices.



Learning Approach and Balance

The module is designed to maintain a strong balance between conceptual understanding and practical application:

- 40% conceptual input, focused on frameworks, policy context and analytical tools
- 60% interactive and applied learning, including discussions, group work and simulation exercises

This approach ensures a high level of participant engagement and facilitates the translation of knowledge into actionable policy insights and institutional practices.



8. Cross-Cutting Integration

This module is fully aligned with:

- EU Integration: alignment with EU cybersecurity and digital policy frameworks
- Common Regional Market (CRM): secure functioning of cross-border systems
- Rule of Law: accountability, transparency and institutional responsibility
- Digital Transformation: cybersecurity as a precondition for digitalization

9. Expected Impact

The module contributes to:

- strengthening policy-level understanding of cybersecurity
- improving institutional preparedness and coordination
- supporting secure implementation of the CRM
- enhancing regional cooperation and resilience
- advancing alignment with EU standards

ANNEX I
Background Material
Cybersecurity, Digital Integration and Regional Cooperation in the Western Balkans

1. Cybersecurity as a Governance Issue

In recent years, cybersecurity has moved beyond the realm of technical systems and specialised IT functions, becoming a central concern for governance, public administration and economic stability. As governments across the Western Balkans increasingly rely on digital systems to deliver services, manage data and enable economic activity, vulnerabilities in these systems translate directly into risks for state functionality.

This risk is no longer theoretical. Western Balkan countries have seen a significant increase in reported cyber incidents since 2020, in line with accelerated digitalization during and after COVID-19. Public institutions remain primary targets, reflecting both their critical role and often limited cybersecurity capacity. In 2022, Albania and Montenegro were targeted by cyberattacks

that affected government networks and required international assistance.

More broadly, according to ENISA, ransomware and distributed denial-of-service (DDoS) attacks remain among the most frequent threats in Europe, with public administration and critical infrastructure among the most targeted sectors. The World Economic Forum consistently ranks cyber insecurity among the top global risks in terms of likelihood and impact, particularly for countries undergoing rapid digital transformation with uneven resilience capacities - such as those in the Western Balkans. Moreover, the cost of cyber incidents is rising globally, with estimates suggesting that cybercrime could reach over $10 trillion annually by 2025, affecting both governments and private sector actors.

Disruptions to digital platforms can affect the delivery of essential public services, undermine institutional credibility and erode citizen trust. At the same time, cyber incidents targeting businesses or financial systems can disrupt economic transactions and weaken market confidence. In this sense, cybersecurity is no longer simply about protecting infrastructure; it is about ensuring the continuity, reliability and legitimacy of governance systems.

This shift requires a corresponding change in how cybersecurity is approached. Rather than being treated as a technical issue managed in isolation, it must be understood as a policy and governance challenge, involving decision-making, coordination and accountability at the highest levels of public administration.

2. Cyber Risks in an Increasingly Inter-connected Region

The Western Balkans face a complex and evolving cyber risk landscape. While digital transformation is advancing, driven by e-government services, digital business models and regional integration initiatives, it is simultaneously increasing systemic exposure to cyber threats.

This exposure is already visible in practice. The 2022 cyberattacks in Albania and Montenegro demonstrated how attacks on government infrastructure can disrupt core administrative functions, disable digital services and require external intervention to restore systems. These incidents highlighted structural vulnerabilities, including dependence on centralized digital platforms and limited redundancy mechanisms.



At the structural level, several risk factors persist across the region:

- Legacy IT systems still in use within public administration, often not aligned with current security standards
- Fragmented governance frameworks, where responsibilities for cybersecurity are split across institutions with limited coordination
- Capacity gaps, including shortages of specialized staff and uneven institutional preparedness

At the same time, the expansion of digital public services and cross-border systems is increasing the scale of potential impact. Cyber incidents are no

longer isolated events; they can trigger cascading effects across sectors. For example:

- A ransomware attack on a public administration database can disrupt civil registries, tax systems or customs operations
- A breach in financial systems can affect payment flows and business transactions
- Disruptions in digital infrastructure can halt e-services relied upon by citizens and companies on a daily basis



Crucially, these risks are increasingly transnational. As the region moves toward deeper economic integration through initiatives such as the Common Regional Market, digital systems are becoming interconnected, particularly in areas such as:

- customs and trade facilitation systems
- data exchange between administrations
- digital certificates and services enabling cross-border mobility

In this context, a vulnerability in one country can directly affect others. A disruption in one node of the system, such as customs IT infrastructure or cross-border data exchange platforms, can slow down or block regional flows of goods, services and information.

This interconnectedness transforms cybersecurity from a national technical issue into a shared regional risk. It requires not only stronger national systems, but also coordination, information-sharing and aligned standards across the region, particularly in view of gradual integration into the EU Single Market.

3. Cybersecurity and the Common Regional Market

The establishment of the Common Regional Market (CRM) represents a key step towards deeper economic integration in the Western Balkans. Its effective functioning increasingly depends on digital systems that enable cross-border services, facilitate trade and support the mobility of people, goods and businesses. In practice, the CRM is not only a policy framework, it is an operational digital ecosystem. Core components of its implementation rely on interconnected systems, including:

- electronic customs and trade facilitation platforms
- business registration and company data exchange systems
- electronic identification and trust services (eID, e-signatures)
- digital certificates and documentation for cross-border movement of goods and services
- financial systems supporting cross-border payments and transactions

This growing reliance on digital infrastructure creates new dependencies and systemic risks. Many of these systems are either already interconnected or are being aligned to enable interoperability across the region. As a result, they form a shared operational space, where disruptions are no longer contained within national borders.

The implications are concrete and immediate. A

cyber incident affecting one component of this ecosystem can generate spillover effects across multiple countries and sectors. For example:

- A disruption in customs IT systems can delay or block cross-border trade flows, affecting supply chains regionally
- A breach in business registries or data exchange platforms can undermine legal certainty and trust for investors and companies
- Compromise of digital certificates or e-signature systems can invalidate transactions and administrative procedures across borders
- Attacks on financial infrastructure can interrupt payment systems and cross-border economic activity

In this context, cybersecurity becomes a functional prerequisite for CRM implementation, not an auxiliary concern. The effectiveness of regional integration depends on the security, reliability and mutual trust in the systems that underpin it. Without this, key CRM objectives, such as seamless trade, mobility and service provision, cannot be fully realised.

This creates a clear policy implication: cybersecurity must be integrated into the design and implementation of the CRM through:

- minimum regional security standards and alignment with EU frameworks (e.g. risk management, incident reporting, critical infrastructure protection)
- mechanisms for cross-border coordination and information sharing
- joint preparedness and response capacities for cyber incidents affecting regional systems
- building trust through interoperable and secure digital services

Ultimately, as the Western Balkans move towards gradual integration into the EU Single Market, the resilience of shared digital systems will determine not only the efficiency, but also the credibility and sustainability of the integration process itself.

4. EU Frameworks and the Changing Nature of Integration



Cybersecurity is also becoming increasingly central to the European Union's policy framework. Through instruments such as the NIS2 Directive and the Cyber Resilience Act, the **European Union has established a more comprehensive and binding approach to the protection of digital systems and services.

These frameworks extend beyond technical standards, introducing requirements related to risk management, institutional responsibilities, incident reporting and cross-border cooperation. For countries aspiring to EU membership, alignment with these frameworks is not only a legal obligation, but also an institutional and operational challenge.

This reflects a broader evolution in the enlargement process. Integration is no longer understood solely as a formal step that follows full compliance. Instead, it increasingly involves

the gradual alignment of systems, practices and institutions with EU standards, allowing for earlier and more practical forms of integration.

This shift is particularly relevant in the digital domain, where participation in cross-border systems and services increasingly depends on the existence of secure, resilient and trustworthy digital infrastructures. As candidate countries move towards deeper involvement in the Common Regional Market and emerging forms of gradual integration into the EU Single Market, cybersecurity becomes not only a matter of regulatory compliance, but also a prerequisite for effective participation.



Consequently, the central challenge for the Western Balkans extends beyond the transposition of EU legislation. It increasingly concerns the development of institutional capacities, coordination mechanisms and governance arrangements capable of implementing EU requirements and sustaining participation in interconnected European digital ecosystems. In this sense, cybersecurity provides a concrete illustration of the broader shift in the enlargement process from a focus on legislative approximation towards a stronger emphasis on institutional readiness and implementation capacity.

5. The Growth Plan and Gradual Integration in the Digital Domain

The EU Growth Plan for the Western Balkans reflects an increasingly operational approach to enlargement, centred on the principle of gradual integration into selected areas of the EU Single Market. Within this evolving framework, the digital domain has emerged as one of the most advanced and tangible areas for early integration.

Building on the objectives of the Common Regional Market, initiatives related to digital identity, payment systems, interoperability and regulatory alignment seek to facilitate the progressive integration of the Western Balkans into European digital frameworks even before full membership. These developments create concrete opportunities for citizens, businesses and public administrations, while simultaneously accelerating reform and convergence processes across the region.

However, participation in such frameworks depends not only on legislative alignment but also on the existence of secure, resilient and trustworthy digital systems. Cross-border digital interactions require confidence in the ability of participating countries to manage cyber risks, protect critical services and ensure the continuity and integrity of digital operations.

In this context, cybersecurity is no longer merely a defensive or technical function. It becomes an enabling condition for regional cooperation and a prerequisite for meaningful participation in emerging forms of gradual integration. Strengthening cybersecurity governance, institutional coordination and resilience is therefore essential not only for protecting digital infrastructures, but also for supporting the credibility and sustainability of the Western Balkans' integration into European digital and economic structures.

6. Digital Trust, Data Protection and Institutional Accountability

At the heart of digital transformation and integration lies the concept of trust. Citizens and businesses must have confidence that digital systems are secure, that their personal and sensitive data is adequately protected, and that institutions possess the capacity to manage digital risks in a responsible and transparent manner.

Digital trust is therefore closely linked to effective data protection frameworks, clear accountability mechanisms and institutional integrity. In the event of a cyber incident, the way institutions respond, including how they communicate, manage information and assume responsibility, can significantly influence public confidence and the perceived legitimacy of public authorities.

In this sense, cybersecurity extends beyond the protection of technological assets and intersects with broader principles of the rule of law. It raises important questions regarding institutional responsibility, oversight, transparency and the safeguarding of rights in increasingly digitalized environments.

For the Western Balkans, where digital transformation, regional cooperation and gradual integration into European frameworks are advancing simultaneously, maintaining high standards of trust and accountability becomes particularly important. Secure and trustworthy institutions are essential not only for effective domestic governance, but also for strengthening confidence in cross-border digital interactions and supporting the credibility of the region's European integration efforts.

7. The Need for Regional Coordination

Given the cross-border nature of cyber risks and the growing interconnectedness of digital systems, no country can effectively address cybersecurity challenges in isolation. The increasing integration of markets, services and digital infrastructures requires approaches that extend beyond national boundaries and involve coordinated action across institutions, sectors and countries.



In the Western Balkans, this reality presents both opportunities and challenges. The implementation of the Common Regional Market and the broader objective of gradual integration into European frameworks depend, to an increasing extent, on the reliability and security of shared and interconnected systems. At the same time, differences in institutional capacities, governance arrangements and levels of preparedness across the region may complicate collective responses to cyber incidents.

These circumstances reinforce the need for stronger regional coordination mechanisms. Information sharing, mutual learning, joint preparedness activities and the development of common approaches can contribute to building trust and enhancing the region's collective ability to prevent, respond to and recover from cyber disruptions.

Regional cooperation in cybersecurity should therefore be understood not only as a security imperative, but also as an enabling factor for

deeper economic integration and more effective participation in emerging forms of gradual integration with the European Union. Strengthening regional resilience ultimately requires a shared recognition that cybersecurity is a common responsibility and that vulnerabilities affecting one country may have implications for the region as a whole.

8. From Risk Management to Resilience

The evolving nature of cyber threats is reshaping approaches to cybersecurity governance. Rather than focusing exclusively on the prevention of incidents or reactive responses once disruptions occur, increasing emphasis is being placed on building resilience.



In this context, resilience refers to the ability of institutions and systems to anticipate, withstand, respond to, adapt to and recover from cyber incidents while maintaining the continuity of essential functions and public services. Building resilience therefore requires a shift from short-term, incident-driven approaches towards longer-term investments in preparedness, coordination and institutional capacity.

Strengthening resilience involves a combination of risk-informed decision-making, preparedness planning, clear governance arrangements and effective coordination mechanisms. It also requires a commitment to continuous learning, enabling institutions to draw lessons from previous incidents and translating them into improved policies, procedures and practices.

Public-private cooperation represents another critical dimension of resilience, recognizing that many essential services and digital infrastructures are operated by, or depend upon, private actors. Similarly, regional cooperation is increasingly important in addressing shared vulnerabilities, enhancing preparedness and strengthening collective capacities to respond to cyber disruptions with cross-border implications.

Ultimately, resilience cannot be developed during a crisis. It is the product of sustained efforts, institutional commitment and strategic investment over time. For the Western Balkans, strengthening cyber resilience is not only essential for effective governance and the protection of critical services, but also for supporting regional cooperation and building the institutional readiness required for deeper integration into European frameworks.

ANNEX II: Key References

Purpose

The following background materials provide the policy, legal and institutional context supporting this training module. They are intended to help participants better understand the evolution of European cybersecurity policy, the implications for EU candidate countries and the relevance of cybersecurity for the implementation of the Common Regional Market (CRM) and the gradual integration of the Western Balkans into the European Union.

Participants are not expected to study all documents in detail. The list is intended as a reference resource before, during and after the training.

PART I
EU Cybersecurity Legislative Framework
Directive (EU) 2022/2555 (NIS2 Directive)

Purpose

The NIS2 Directive establishes the core European framework for cybersecurity governance. It significantly expands the scope of the original NIS Directive by introducing stronger governance requirements, clearer institutional responsibilities, mandatory cybersecurity risk management measures and harmonised incident reporting obligations across Member States.

Participants should understand

- why cybersecurity has become a governance responsibility rather than only an IT issue;
- the distinction between essential and important entities;
- governance responsibilities of public authorities;
- risk management obligations;
- incident notification requirements;
- supervisory mechanisms;
- cross-border cooperation.

Relevance for the Western Balkans

NIS2 represents one of the principal areas of future legislative approximation for candidate countries. Beyond legal alignment, it requires institutional capacity, coordination mechanisms and implementation capabilities.



Regulation (EU) 2024/2847 – Cyber Resilience Act

Purpose

The Cyber Resilience Act establishes horizontal cybersecurity requirements for products with digital elements throughout their lifecycle.

It introduces a preventive approach to cybersecurity by requiring manufacturers to integrate cybersecurity into product design, maintenance and vulnerability management.

Participants should understand

- secure-by-design principles;
- cybersecurity obligations throughout product lifecycles;
- vulnerability handling;
- conformity assessment;
- market surveillance.

Relevance

Although primarily addressing manufacturers and digital markets, the Act demonstrates how cybersecurity increasingly influences the functioning of the Single Market.

Regulation (EU) 2025/38 – Cyber Solidarity Act

Purpose

The Cyber Solidarity Act strengthens European preparedness against large-scale cyber incidents.

It creates mechanisms for:



- coordinated preparedness;
- mutual assistance;
- cyber emergency support;
- large-scale incident response;
- European Cyber Shield.

Participants should understand

- why cyber crises require coordinated responses;
- the importance of operational cooperation;
- the evolution towards European cyber solidarity.

PART II
EU Digital Policy Framework
EU Cybersecurity Strategy for the Digital Decade (2020)

The Strategy sets out the European Union's long-term vision for achieving an open, secure and resilient cyberspace.

Key themes include:

- resilience;
- technological sovereignty;
- cyber diplomacy;
- operational cooperation;
- international partnerships.

Digital Decade Policy Programme 2030

The Digital Decade establishes strategic objectives for Europe's digital transformation, including:

- digital public services;
- digital infrastructure;
- digital skills;
- digital businesses.

Participants should understand that cybersecurity underpins each of these priorities.

European Digital Identity Framework

The framework supports interoperable electronic identification across Europe.

Topics include:

- European Digital Identity Wallet;
- trust services;
- electronic identification;
- interoperability.



European Strategy for Data

Explains how Europe seeks to develop a trusted data economy while ensuring:

- privacy;
- security;
- interoperability;
- data governance.

Artificial Intelligence Act

Participants should appreciate the relationship between:

- AI governance;
- trustworthy AI;
- cybersecurity;
- data governance;
- institutional accountability.

PART III
Enlargement and Regional Integration
EU Growth Plan for the Western Balkans



Participants should understand:

- gradual integration;
- phased access to the Single Market;
- Reform Agendas;
- Reform and Growth Facility;
- performance-based financing.

Special attention should be given to the digital dimension of gradual integration.

Reform and Growth Facility

Focus on:

- reform implementation;
- conditionality;
- institutional capacity;
- monitoring mechanisms.

Common Regional Market (CRM)

Participants should understand how cybersecurity supports:

- trade facilitation;
- digital services;
- interoperability;
- cross-border cooperation;
- digital mobility.

Digital Agenda for the Western Balkans

The Digital Agenda provides the regional policy framework supporting:

- broadband deployment;
- cybersecurity;
- digital public services;
- digital skills;
- trust services.

PART IV
European Cybersecurity Governance

Participants are encouraged to familiarize themselves with the mandates of the following institutions.

European Union Agency for Cybersecurity (ENISA)

Topics:

- threat landscape;
- policy guidance;
- NIS2 implementation;
- cyber exercises;
- capacity building.

CSIRTs Network

Purpose:

- operational cooperation;
- information exchange;
- incident coordination.

EU-CyCLONe

Focus:

- management of large-scale cyber crises;
- strategic coordination;
- political decision support.



European Cybersecurity Competence Centre (ECCC)

Role:

- research;
- innovation;
- cybersecurity capacity building.

DG CONNECT

Responsible for:

- digital policy;
- cybersecurity legislation;
- Digital Decade implementation.

PART V
Recommended Case Studies

Participants are encouraged to analyse selected cases discussed during the training.

Suggested examples include:

- Albania cyberattack (2022)
- Montenegro cyberattack (2022)
- Colonial Pipeline ransomware attack
- SolarWinds supply-chain compromise
- WannaCry ransomware outbreak
- NotPetya cyberattack
- Microsoft Exchange Server attacks
- CrowdStrike global IT disruption (2024)

Each case should be analysed from a governance perspective, examining:

- institutional preparedness;
- decision-making;
- crisis coordination;
- communication;
- continuity of services;
- lessons learned.



PART VI
Suggested Pre-Course Reading

Participants are encouraged to review the following documents before attending the training:

Essential

- Executive Summary of the NIS2 Directive
- EU Growth Plan for the Western Balkans
- Common Regional Market Action Plan
- ENISA Threat Landscape Executive Summary
- Digital Decade Policy Programme 2030

Recommended

- Cyber Resilience Act
- Cyber Solidarity Act
- EU Cybersecurity Strategy
- OECD Digital Security Recommendation
- World Economic Forum Global Cybersecurity Outlook



