Module	**Cybersecurity**
Jurisdictions	**European Union**

Module Scope

Does your organisation understand the legal and regulatory obligations it must comply with in relation to cybersecurity, digital operational resilience and data protection under European Union law?

Does your organisation understand the governance, risk management and technical measures required to ensure the security of network and information systems, products with digital elements and critical infrastructure?

Does your organisation understand how to navigate and comply with the framework of legislative and compliance requirements governing cybersecurity risk management, incident response, supply chain security and reporting obligations across the European Union?

Module Application

The EU CYBERSECURITY module provides information to organisations about how to comply with legal responsibilities when dealing with the following:

- Governance and accountability for cybersecurity and digital resilience
- Cybersecurity risk management frameworks and policies
- Incident detection, response, and notification obligations
- Supply chain and third-party risk management
- Security requirements for network and information systems
- Protection of personal data and privacy
- Security of products with digital elements
- Business continuity and operational resilience
- Critical infrastructure and essential service resilience
- Regulatory reporting and supervisory engagement

The EU CYBERSECURITY module also comprehensively covers requirements arising under key European Union instruments, including:

- Network and information security obligations (including NIS2 framework)
- Digital operational resilience requirements for financial entities
- Cybersecurity requirements for digital products and software
- Protection of critical entities and infrastructure
- Personal data protection and breach notification obligations

Organisations, their employees, and responsible officers are expected to be familiar with the broad landscape of cybersecurity and data protection obligations to which they are subject, as well as the more specific obligations relevant to their sector, size and risk profile.

The EU CYBERSECURITY module should be subscribed to by any organisation that:

- Operates within the European Union
- Provides digital services, ICT systems, or data-driven products
- Is classified as an essential or important entity, or
- Is otherwise subject to EU cybersecurity, resilience, or data protection laws

The aim of the module is to equip subscribers with knowledge of their obligations under EU law and the systems and processes that should be implemented to ensure an effective cybersecurity and compliance management framework.

The specific questions and answers covered by the module include:

- How to establish governance structures and assign accountability for cybersecurity compliance
- How to implement and maintain cybersecurity risk management frameworks
- How to develop and enforce cybersecurity policies and procedures
- How to identify, assess, and manage ICT and cybersecurity risks
- How to detect, respond to, and recover from cybersecurity incidents
- How to comply with incident notification and reporting requirements
- How to manage cybersecurity risks arising from third-party suppliers and service providers
- How to ensure security in the design, development, and maintenance of digital products
- How to comply with personal data protection and breach notification obligations
- How to implement business continuity and disaster recovery plans
- How to prepare for regulatory supervision, audits and inspections
- How to build organisational resilience against cyber threats and disruptions

The EU CYBERSECURITY module covers an organisation's obligations across the full cybersecurity lifecycle, including governance, prevention, detection, response and recovery. It incorporates relevant international standards and best practice frameworks to demonstrate practical steps organisations can take to meet their obligations through the implementation and maintenance of robust internal processes.

Significant penalties may be imposed if an organisation fails to comply with its legislative obligations. These penalties may include substantial administrative fines, regulatory enforcement actions, and, in some cases, personal liability for management bodies and senior officers. The range of consequences is discussed in detail throughout the module.

The EU CYBERSECURITY module focuses on the role and responsibilities of organisations. It does not cover the role or actions to be taken by individual consumers in the event of a cybersecurity incident or regulatory breach.

About LexisNexis Regulatory Compliance

LexisNexis Regulatory Compliance® helps you forge a clear path to compliance.

With LexisNexis® content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.