Global Cybersecurity

Module application

Does your organisation understand the legal and regulatory international cybersecurity obligations they must comply with?

Is your organisation required to comply with data risk assessment and management requirements and procedures?

Does your organisation understand how to navigate and comply with fundamental legislative and compliance requirements that surround the cybersecurity framework when using data internationally for example privacy data policies?

Module scope

The GLOBAL CYBERSECURITY module provides information to organisations in how to apply comply with legal responsibilities when doing the following:

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management
- Identity Management, Authentication and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes
- Maintenance
- Protective Technologies
- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes
- Response Planning
- Communication
- Mitigation
- Improvement of Response Activities
- Recovery Planning
- Recovery Communications

Organisations, their employees, and authorised individuals are all expected to be familiar with the broad landscape of legal and regulatory obligations to which they are subject as well as more specific obligations relevant to the particular sector in which they are operating. The GLOBAL CYBERSECURITY module should be subscribed to by every organisation who is involved with digital data. The aim of the module is to equip the subscriber with knowledge of their requirements under the international cybersecurity laws and the relevant systems and processes that should be implemented to ensure an effective compliance management system within the organisation.

The specific questions and answers covered by the module are:

- How to implement an asset management process to defend the organisation's data and digital processes from intruders
- How to collect and document a range of data that will serve as inputs to the organisation's risk management process
- How to incorporate digital security into the organisation's governance processes
- How to conduct a risk assessment process to determine digital security risks and to identify available responses
- How to establish a risk management strategy to govern the deployment of digital security controls
- How to address and manages cyber supply chain risks by performing risk assessments, designing contract provisions, conducting audits, and creating response and contingency plans
- How to implement authentication processes and security measures to control access to information systems
- How to provide digital security training activities to all personnel to equip them with the required knowledge and skills
- How to implement security measures to protect the confidentiality and integrity of data, digital services and information systems
- How to establish security policies, procedures and systems that are necessary to protect digital assets and information
- How to establish processes designed to ensure the security of information systems undergoing maintenance or repair
- How to deploy technological security measures and controls designed to protect stored data, network integrity and critical digital services
- How to detect network anomalies, identify the events causing the anomalies, assesses the harm caused by anomalous events, and triggers incident response measures when appropriate
- How to monitor information system assets, network traffic and the activities of personnel to detect potential cybersecurity events
- How to implement processes to assist in detecting any potential cybersecurity events
- How to develop and execute effective response planning mechanisms
- How to conduct a thorough analysis of any incidents that occur and implement processes to prevent such incidents from occurring in the future

- How to prevent, mitigate and resolve any incidents that occur, and mitigate or document any new vulnerabilities
- How to ensure that the organisation's response activities are improved by incorporating lessons from other detection and response activities
- How to ensure that the organisation's recovery processes and procedures are executed and maintained so that all systems and assets are restored, and that they are improved by incorporating lessons learned into future activities
- How to coordinate the organisation's restoration activities with internal and external parties

The GLOBAL CYBERSECURITY module covers all an organisation's obligations for protecting systems and data including the application of the National Institute of Standards and demonstrates practical assistance and guidance to ensure that these obligations are complied with through the implementation and maintenance of best practice processes throughout the organisation.

If the organisation fails to take all reasonable steps to secure digital information and systems, then it may result in the organisation becoming liable to compensate individuals and organisation that incur losses as a result of a security breach. Significantly large penalties can also be imposed if the organisation fails to meet the legislative obligations. Such penalties can include pecuniary penalties, enforcement actions, compliance, and compensation orders. The range of consequences that may be imposed on organisations is discussed in detail in this module.

The GLOBAL CYBERSECURITY module covers the role and responsibilities of an organisation. It does not cover the role or actions to be taken by consumers in the event of a breach of regulations or obligations by an organisation.

LexisNexis Regulatory Compliance is a legal obligations register and alerting solution that combines regulatory content with technology to empower you to take control of your compliance obligations.