**CYBERYOUTH**

**Nonformal education for cyber-security training & resilience of youth organisations and young people**

***Cybersecurity online youth academy***

****

**Governance, Risk and Compliance**

Table of contents

[Introduction](#_heading=h.fpb3yt6tcffi)

[It could have happened to you…](#_heading=h.c7zxm1r80lor)

[What you will learn](#_heading=h.bd1t10x6k115)

[Why it is important](#_heading=h.1fqj6c1n3ygs)

[How it can help you in everyday life](#_heading=h.bddh90wxykhs)

[What career you can pursue](#_heading=h.l25siuf1d90q)

[Pre-requisites](#_heading=h.obikvf4haym5)

[Material](#_heading=h.snpqznqbwxs)

[6.1 Legislation and Regulation](#_heading=h.2yz7x8bu8zb5)

[Data Protection Legislation](#_heading=h.oo7qhy4nz301)

[GDPR](#_heading=h.mxx776cq98gz)

[European Legislation](#_heading=h.gpht6cntx8cg)

[National/State Legislation](#_heading=h.jo5y0jx0953s)

[Conclusions](#_heading=h.q7y4utybp22l)

[6.2 Key Data Protection Frameworks](#_heading=h.wv8lmqsplpdd)

[ISO](#_heading=h.se3v82rotiu3)

[CSF](#_heading=h.xa9iyn2x8esy)

[6.3 Personnel Management](#_heading=h.g98km9urykdd)

[Personnel Introduction](#_heading=h.d7j3sia9a2ue)

[Onboarding](#_heading=h.4rgr0sqkydi2)

[Basic Security Policy](#_heading=h.yqucjs90vwi5)

[Training](#_heading=h.uu16mwe9cyzf)

[Conduct and Behaviour Policies](#_heading=h.aymlrjsxfl61)

[Internal Risk Management](#_heading=h.ls5c88is89uy)

[6.4 Third-Party Risk Management](#_heading=h.7pii0khen2cd)

[Conclusions](#_heading=h.8fgh3pvuc4s3)

[6.5 Sensitive Data](#_heading=h.azw51npc11fy)

[Conclusions](#_heading=h.scbfee5behhv)

[The Geek’s Corner](#_heading=h.floxyjcfjlz3)

[Conclusions](#_heading=h.umqq3lf4f2yk)

[Quiz](#_heading=h.35btfg6prjdy)

[References](#_heading=h.ioedg3ublhq7)

# 

# **Introduction**

## **It could have happened to you…**

In 2022, the NHS, the UK’s socialised healthcare system, suffered a phishing attack that led to hundreds of employee emails and personal data being made available and to a data breach in the internal system.

Employees were found to have received a fake login request to their internal accounts, which by logging into these accounts, allowed malicious attackers to gain access to their accounts and access privileged information without any issue at all.

Unfortunately, situations like this one (attacks due to human error or improper training) are far more common than the type of cyberattack shown in media such as TV or movies, which is why the importance of proper onboarding and personnel training, as well as strict data policies, can’t be overstated.

Maybe you should think twice when you get an email from a company claiming that you must log in right now!

## **What you will learn**

In this module, we will learn about the legal and governmental restrictions to keep data, and therefore people, safe, as well as learning more regarding risk assessment and management, from personnel training all the way to the treatment of highly sensitive data, as well as the process involved in identifying and acting upon these risks and preventing risks from becoming incidents, or incidents from becoming crises. We will discuss some of the key frameworks and standards involved in the exchange and treatment of data, both historically, and most of all, currently. During this module, a key aspect to take into account, and perhaps the most important and often ignored; **compliance**. After all, we can develop the safest scheme or policy possible, but without compliance, that all goes out of the window!

## **Why it is important**

This module is essential for you and your organisation as it provides a foundation for understanding the importance of data governance and the compliance of set guidelines, laws and regulations in mitigating cybersecurity risks that can endanger organisational and personal data. Through the completion of this module, we will understand the risks undergone when dealing with personal or sensitive data, and through this, the importance of regulations and governance to dictate how this is done. After all, these laws or regulations may seem unnecessary at first glance, but they are the key to making sure all organisations and/or businesses follow strict guidelines instead of leaving these decisions to personal opinion.

## **How it can help you in everyday life**

The materials covered in this module may not seem it at first, but they are key to keeping data safe and collaborating with the set standards in data protection, as well as understanding *why* they exist in the first place, gaining stronger knowledge in digital and physical data governance, as well as the significance of compliance with local, national and international guidelines and legal frameworks, learning how we can reduce the risk of incidence and security breaches or issues by following and complying with the established laws, as well as keeping records and documentation of frameworks being followed to ensure being legally covered in case of incidence or any form of cyber attack.

## **What career you can pursue**

Through completing this module and the online course in general, you will learn more regarding the intricacies of data regulation and compliance, as well as the risks associated with not following these, whilst gaining further knowledge regarding the key points in onboarding and preparation of new employees, preparing you for such positions such as:

* Onboarding Specialist
* Risk Assessment Agent
* Junior Regulation Expert

## **Pre-requisites**

To fully benefit from the content of this module, we recommend completing the previous modules of the online course to follow the common important threads and better understand the concepts discussed. You won’t need any prior knowledge on data regulation other than a basic familiarity with the concepts, so this module is great to learn from scratch, or to improve your existing knowledge.

# 

# 

# 

# **Material**

## **6.1 Legislation and Regulation**

### Data Protection Legislation

One of the keys to digital safety is regulating data protection to standardize the way data is treated. In this way, data protection legislation exists and is implemented to regularize the ways that data can be dealt with.

### GDPR

Anyone working in the cybersecurity industry must be familiar with the General Data Protection Regulation (GDPR). A comprehensive data protection framework called GDPR was put into effect in 2018 with the aim of preserving people's right to privacy inside the European Union (EU). It lays up a number of guidelines, requirements, and rights pertaining to the gathering, handling, and storing of personal data. You must understand the fundamental ideas of GDPR as a cybersecurity expert, including the notions of lawfulness, fairness, and transparency, as well as data subject rights, organizational responsibilities, and the penalties for non-compliance.

Understanding GDPR can help you improve data security and privacy for both individuals and enterprises by giving you useful insights into the protection of personal data and ensuring that your cybersecurity activities comply with the legal standards.

### European Legislation

The development of cybersecurity methods and the protection of data privacy are significantly influenced by European legislation. Cybersecurity experts should be conversant with other significant laws and directives inside the European Union in addition to GDPR. Operators of vital services and digital service providers must adhere to the Network and Information Security Directive's (NIS Directive) criteria for cybersecurity and incident reporting. It attempts to increase the overall resilience of crucial internet services and infrastructure.

The ePrivacy Directive is focused on ensuring the privacy of those who use electronic communications, and it contains regulations governing cookies, marketing messages, and the confidentiality of such data. The EU Cybersecurity Act also creates a framework for the accreditation of cybersecurity-related goods, services, and procedures. Cybersecurity experts may maintain compliance and help create a safe and privacy-respecting digital environment inside the European Union by remaining knowledgeable on European legislation.

### National/State Legislation

In addition to European legislation, it is crucial for cybersecurity professionals to understand national regulations governing data protection and cybersecurity practices. Each country within the European Union may have its own specific laws and regulations that complement GDPR and provide further guidance on cybersecurity obligations. For example, in the United Kingdom, the Data Protection Act 2018 supplements GDPR and outlines additional requirements for data protection. Similarly, countries like Germany, France, and Spain have implemented their own national laws to supplement and clarify GDPR provisions.

These national regulations may address specific areas such as data breach notification requirements, sector-specific regulations, or additional safeguards for personal data processing. As a cybersecurity professional, staying up to date with national regulations is vital to ensure compliance and effectively protect data within specific national jurisdictions. By understanding both European and national legislation, cybersecurity professionals can navigate the complex regulatory landscape and implement robust cybersecurity measures that align with both regional and local requirements.

In all cases regarding cybersecurity and regulation, it is key to consult your national, regional and local legal frameworks to understand how it varies compared to EU regulation and GDPR to comprehend how to properly comply with regulations around the EU and local levels.

### **Conclusions**

To sum up what we have discussed, the EU is leading the way worldwide in the safety of personal data and the right to privacy in an increasingly public world. Data regulations such as GDPR are key in maintaining online safety and privacy for the entire population, and compliance with them is key to treating data ethically, legally and responsibly. Though GDPR guidelines are strict and clear, they may be enforced more or less in certain countries, therefore it is always important to be as cautious and respectful of privacy as possible, while understanding the legal grounds in an organisation’s country to have better knowledge on the treatment of data.

## **6.2 Key Data Protection Frameworks**

With the importance of data safety and the protection of sensitive or personal information, the usage of standardized guidelines beyond the legal frameworks implemented at a national or European level has become more commonplace in many organisations and companies. Let’s take a look at two key frameworks dealing with risk management and data protection for organisations as well as individuals.

### **ISO**

The ISO (International Organization for Standardization) framework is a set of international standards that provides guidelines and best practices for various aspects of organizational management, including cybersecurity. Here are some key points about the ISO framework:

1. **ISO 27001: Information Security Management System (ISMS)**: ISO 27001 is the leading standard for information security management. It provides a systematic approach for establishing, implementing, maintaining, and continually improving an organization's ISMS. The standard encompasses various security controls and risk management processes to protect the confidentiality, integrity, and availability of information.
2. **ISO 27002: Code of Practice for Information Security Controls**: ISO 27002 provides a comprehensive set of security controls that can be implemented to address specific information security risks. It offers guidance on the selection, implementation, and management of controls across various domains such as access control, cryptography, physical security, incident management, and more.
3. **ISO 27005: Information Security Risk Management**: ISO 27005 focuses on the systematic management of information security risks within an organization. It provides guidelines for risk assessment, risk treatment, and risk acceptance processes. The standard emphasizes the importance of identifying and evaluating risks to make informed decisions regarding the implementation of security controls.
4. **ISO 31000: Risk Management**: ISO 31000 is a broader risk management standard applicable to various domains, including cybersecurity. It provides principles, framework, and processes for managing risks effectively. While ISO 27005 focuses specifically on information security risks, ISO 31000 provides a more general approach that can be applied to other areas of risk management within an organization.
5. **ISO 22301: Business Continuity Management System (BCMS)**: ISO 22301 focuses on establishing and maintaining a BCMS to ensure organizations can effectively respond and recover from disruptive incidents. It provides a framework for business continuity planning, including risk assessment, business impact analysis, and development of continuity strategies.
6. **ISO 20000: IT Service Management**: ISO 20000 outlines best practices for IT service management, including the delivery, management, and support of IT services. While not specifically focused on cybersecurity, it emphasizes the importance of secure IT service delivery, incident management, and continual improvement of IT processes.

These ISO standards provide organizations with internationally recognized frameworks and guidelines to establish effective cybersecurity and risk management practices. Implementing these standards can help organizations enhance their security posture, demonstrate compliance with industry best practices, and build trust with stakeholders.

### **CSF**

The CSF framework, also known as the NIST Cybersecurity Framework, is a set of guidelines and best practices developed by the National Institute of Standards and Technology (NIST) in the United States. CSF provides a flexible and voluntary framework for organizations to manage and mitigate cybersecurity risks effectively.

The CSF framework consists of three main components: the Core, the Implementation Tiers, and the Profile.

1. Core: The Core of the CSF framework includes five key functions: Identify, Protect, Detect, Respond, and Recover. These functions represent the fundamental cybersecurity activities that organizations should undertake to establish a strong cybersecurity posture. Each function is further divided into categories and subcategories that provide more specific guidance on cybersecurity activities.
2. Implementation Tiers: The Implementation Tiers in the CSF framework provide a way for organizations to assess and communicate their cybersecurity maturity level. There are four tiers: Partial, Risk Informed, Repeatable, and Adaptive. These tiers help organizations understand their current state of cybersecurity and set goals for improvement.
3. Profile: The Profile component of the CSF framework allows organizations to align their cybersecurity activities with their business requirements and risk tolerance. Organizations can create a Profile by selecting the relevant categories and subcategories from the Core based on their specific needs, priorities, and available resources.

The CSF framework emphasizes a risk-based approach to cybersecurity, focusing on continuous improvement and collaboration between different business functions. It provides a common language and framework for organizations to manage and communicate cybersecurity risks effectively, both internally and externally. The CSF framework can be adopted by organizations of any size, sector, or maturity level to enhance their cybersecurity posture and resilience.

## **6.3 Personnel Management**

Another key to regulation and compliance is proper understanding on behalf of members of an organisation. After all, if our team members don’t understand their obligations in dealing with data, how can we expect them to comply? This is where the importance of proper training before starting at a new workplace is key, and why properly preparing new employees or team members is a key pillar in ensuring laws and regulations are followed. As they say, start as you mean to continue!

### **Personnel Introduction**

As mentioned, the key to making sure an organisation is following procedure is to train employees and team members to follow correct procedure from the start. This means making sure that all the rules, regulations or relevant laws are explained and training is facilitated to new members, and ideally, supervision should be offered during a brief period whilst new members familiarize themselves with the organisation and the developments.

#### Onboarding

The most important part of properly preparing a new employee or team member for success, both in a security sense and otherwise, is a detailed and clear onboarding process. In a lot of cases, this can be developed through videos, slideshow presentations, or sometimes even through a brief e-learning experience. Whichever method it is developed with, the key pillars stay the same; the onboarding process should brief a new team member on everything they need to know, as well as offering resources for later consultation, to allow members to integrate seamlessly into an organisation without becoming a risk either for productivity, or more importantly, the organisation’s cybersecurity. A proper onboarding process should leave the employee or team member ready to get started in a safe and responsible manner.

#### Basic Security Policy

As well as preparing members through a detailed onboarding, as we have discussed in previous modules, one of the most crucial points in any organisation’s cybersecurity is to have clear and defined rules and regulations internally, not just legally. Through developing a clear and concise Security Policy, we can ensure conformity throughout the organisation in keeping data safe, as well as making sure employees and team members stay safe in communication.

### **Training**

As well as internal policies and onboarding, it is important to make sure organisation’s members are offered access to consistent and significant training opportunities to build their cybersecurity knowledge and competences within the organisation to guarantee the capacities of team members and workers.

### **Conduct and Behaviour Policies**

In a cybersecurity context, the establishment of robust conduct policies is essential to promote a culture of responsible and secure behavior within an organization. Conduct policies in this context should emphasize the importance of safeguarding sensitive information, protecting systems and networks, and adhering to ethical standards. They should clearly outline guidelines for acceptable use of technology resources, including proper handling of data, adherence to security protocols, and adherence to applicable laws and regulations. Additionally, conduct policies should address the potential risks associated with social engineering, phishing attacks, malware, and other cybersecurity threats. Emphasizing the importance of regular software updates, strong passwords, and the reporting of suspicious activities will help create a security-conscious culture. By establishing and enforcing strong conduct policies, organizations can reduce the likelihood of security incidents and enhance overall cybersecurity posture.

### **Internal Risk Management**

Internal risk management in a cybersecurity context is crucial for organizations to identify, assess, and mitigate potential risks to their information systems and sensitive data. It involves a systematic approach to understanding and managing internal vulnerabilities, threats, and potential impacts on cybersecurity. Effective internal risk management entails conducting regular risk assessments to identify weaknesses, evaluating the likelihood and potential impact of different threats, and prioritizing mitigation efforts accordingly. It also involves establishing robust internal controls, such as access controls, encryption, and monitoring systems, to detect and respond to security incidents promptly. Additionally, organizations need to educate and train their employees on cybersecurity best practices, fostering a culture of awareness and accountability throughout the organization. By implementing a comprehensive internal risk management strategy, organizations can proactively protect their assets, mitigate potential cybersecurity risks, and ensure the continuity of their operations in the face of evolving threats.

## **6.4 Third-Party Risk Management**

Third-party risk management is a critical aspect of cybersecurity as organizations often rely on external vendors, suppliers, and partners who may have access to their systems, networks, or sensitive data. Effective third-party risk management involves assessing and mitigating potential cybersecurity risks associated with these external entities. Organizations should establish a comprehensive framework that includes due diligence processes for evaluating third-party cybersecurity practices, contractual agreements that outline security requirements and responsibilities, and ongoing monitoring and auditing mechanisms to ensure compliance.

To effectively manage third-party risk, organizations should start by identifying and categorizing their critical vendors and partners based on their level of access and the sensitivity of the data they handle. Due diligence should be conducted to evaluate the security controls, policies, and practices of these third parties. This may include reviewing their security certifications, conducting on-site audits, or requesting documentation of their cybersecurity policies and incident response plans. Additionally, organizations should establish clear contractual agreements that outline specific security requirements, data protection measures, incident response protocols, and liability provisions.

Ongoing monitoring and periodic assessments should be conducted to ensure that third parties continue to meet the agreed-upon security standards and to promptly address any identified vulnerabilities or breaches. By implementing a robust third-party risk management program, organizations can strengthen their overall cybersecurity posture and mitigate potential risks introduced by external entities.

In conclusion, third-party risk management is an essential component of cybersecurity. By conducting thorough due diligence, establishing clear contractual agreements, and implementing ongoing monitoring and auditing processes, organizations can effectively assess and mitigate potential cybersecurity risks posed by their external vendors and partners. This proactive approach helps safeguard the organization's systems, networks, and sensitive data, ensuring the overall security and integrity of their operations.

### **Conclusions**

In conclusion, the management, including proper training and onboarding, of team members and employees, is a key point in the security of an organisation and in the compliance with data governance and regulations, along with the safety of customers or users, as well as employees or team members.

## **6.5 Sensitive Data**

Taking all that we’ve discussed into account, we can understand the importance of dealing with data in a proper manner and following governance and legislation detailing the treatment of personal data. So, when dealing with sensitive or potentially harmful data (data including names of underage users, social security details, addresses, passwords, etc.), these rules and regulations should be taken even more to the “letter of the law” so to speak.

Sensitive data management is a critical aspect of cybersecurity as organizations handle vast amounts of confidential and sensitive information. Effectively managing sensitive data involves implementing robust policies, procedures, and safeguards to protect its confidentiality, integrity, and availability. This includes identifying and classifying sensitive data based on its level of sensitivity and potential impact if compromised. Organizations should always develop and implement strict policies including methods previously discussed to keep data safe, such as backups, recoveries, encryption, etc.

### **Conclusions**

To reflect, the treatment of personal data should be treated with extra care, but should follow the same guidelines and laws as the treatment of any data or information.

## **The Geek’s Corner**

Through properly training team members and implementing clear, concise policies on Data Governance complying with the leading guidelines and frameworks, such as GDPR, we can improve an organisation’s security at the most basic level, simply by providing information and training to our employees and or members.

There are many tools and resources available to provide employees, volunteers or group members with training. Unfortunately, data laws are always evolving and changing, so providing specific resources could lead to outdated information. Instead, most organisations recommend providing frequent (once every trimester, for example) and clear training and information on data management best practices, as well as providing examples or cases to avoid, discussing incidents, etc. Some examples of knowledge that isn't affected by changing laws could be key factors such as:

* Do not allow team members to access sensitive data on their personal devices.
* Make sure team members are not exchanging sensitive information unencrypted over external channels.
* Provide risk analysis checks to your team on a regular (bi-annual or more) basis to ensure all data policies are being followed and respected.

# **Conclusions**

In conclusion, the key to Data Governance, as well as Risk Management and Compliance with existing frameworks, is commitment to providing team members with the proper training and understanding of these concepts.

The importance of these concepts in running a digitally safe, responsible and trustworthy organisation is key to the safety of employees, team members, and in the case of many organisations, users/patients.

## **Quiz**

**What is the main purpose of data governance frameworks?**

a) To tell us what to do and boss us around

b) To standardise the way data is treated and the policies toward it.

c) To monitor how people use their systems

d) To make sure no one is able to live offline

**Is GDPR relevant in cybersecurity?**

a) No, it is just brought up so no one complains

b) It’s the leading guideline for data protection in Europe, as well as the world leader.

c) It is important but not as much as National Legislation

d) A method used by hackers to gain access to a system

**How should proper onboarding prepare an employee?**

a) An employee should be ready to integrate seamlessly into the team

b) Tell them where the coffee is

c) They should be given a password and user, everything else is for them to learn

d) They should know the name of the company and their position

**Should sensitive data be treated with different standards?**

a) It should be dealt with through the same standards and guidelines, with extra caution

b) It should be sent unencrypted by email

c) No, it’s the same as any data

d) Yes

**What is the term for a type of cyber attack where an attacker intercepts communication between two parties in order to steal sensitive information?**

a) Man-in-the-Middle (MitM) attack

b) Cross-Site Scripting (XSS) attack

c) Cross-Site Request Forgery (CSRF) attack

d) Ransomware attack

## **References**

United States Securities and Exchange Commission. (2018). Equifax Inc. Form 8-K: Current report filing (Amended). Retrieved from https://www.sec.gov/Archives/edgar/data/33185/000119312518154706/d583804dex991.htm