IT Fundamentals for Cyber Security

Chapter 03: Basics of Cyber Security

Co-funded by
the European Union

Cybersecurity for all (CS4ALL) ERASMUS-EDU-2022-CBHE, No 101083009

Table of Contents

List of figures

3. Basics of Cyber Security

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

3.1. Cybersecurity Principles and Goals

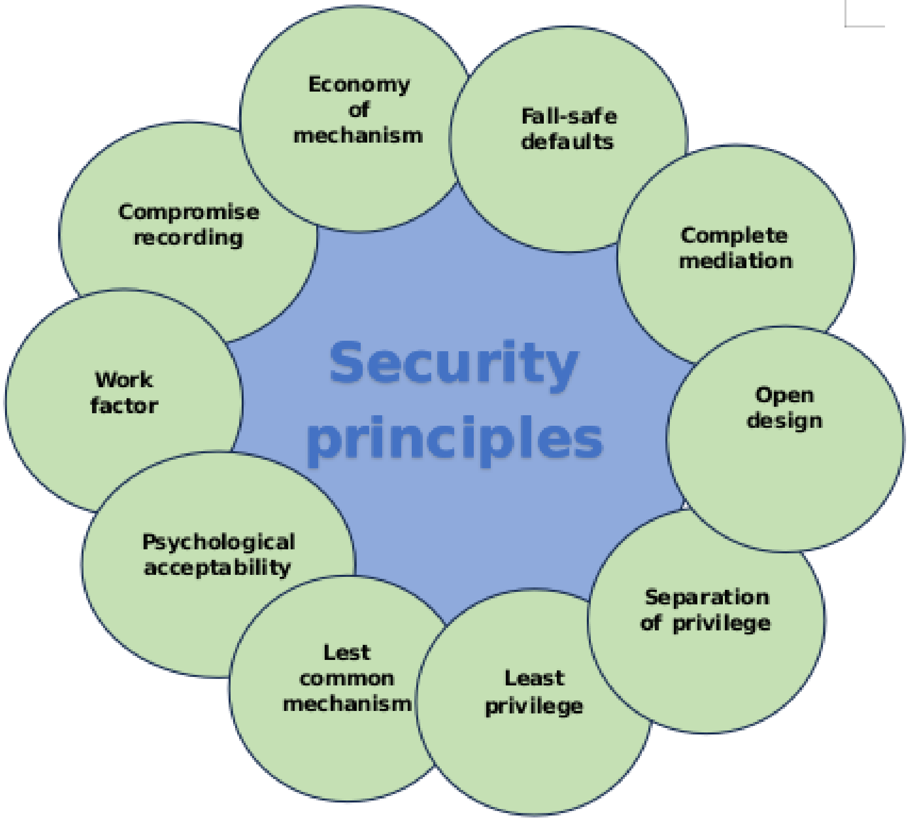


Figure 1. Security Principles

1. Economy of mechanism

This principle states that Security mechanisms should be as simple and small as possible. The Economy of mechanism principle simplifies the design and implementation of security mechanisms. If the design and implementation are simple and small, fewer possibilities exist for errors. The checking and testing process is less complicated so that fewer components need to be tested.

2. Fail-safe defaults

The Fail-safe defaults principle states that the default configuration of a system should have a conservative protection scheme. This principle also restricts how privileges are initialized when a subject or object is created. Whenever access, privileges/rights, or some security-related attribute is not explicitly granted, it should not be grant access to that object.

3. Least Privilege

This principle states that a user should only have those privileges that need to complete his task. Its primary function is to control the assignment of rights granted to the user, not the identity of the user.

4. Open Design

This principle states that the security of a mechanism should not depend on the secrecy of its design or implementation. It suggests that complexity does not add security. This principle is the opposite of the approach known as "security through obscurity." This principle not only applies to information such as passwords or cryptographic systems but also to other computer security related operations.

5. Complete mediation

The principle of complete mediation restricts the caching of information, which often leads to simpler implementations of mechanisms. The idea of this principle is that access to every object must be checked for compliance with a protection scheme to ensure that they are allowed.

6. Separation of Privilege

This principle states that a system should grant access permission based on more than one condition being satisfied. This principle may also be restrictive because it limits access to system entities. Thus before privilege is granted more than two verification should be performed.

7. Least Common Mechanism

This principle states that in systems with multiple users, the mechanisms allowing resources shared by more than one user should be minimized as much as possible. This principle may also be restrictive because it limits the sharing of resources.

8. Psychological acceptability

This principle states that a security mechanism should not make the resource more complicated to access if the security mechanisms were not present. The psychological acceptability principle recognizes the human element in computer security. If security-related software or computer systems are too complicated to configure, maintain, or operate, the user will not employ the necessary security mechanisms.

9. Work Factor

This principle states that the cost of circumventing a security mechanism should be compared with the resources of a potential attacker when designing a security scheme. In some cases, the cost of circumventing ("known as work factor") can be easily calculated.

10. Compromise Recording

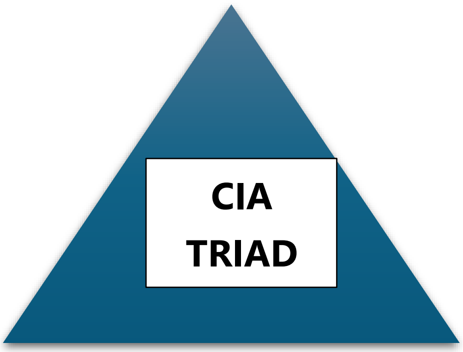
The Compromise Recording principle states that sometimes it is more desirable to record the details of intrusion that to adopt a more sophisticated measure to prevent it.

Cyber Security Goals

The objective of Cybersecurity is to protect information from being stolen, compromised or attacked. Cybersecurity can be measured by at least one of three goals-

1. Protect the confidentiality of data.
2. Preserve the integrity of data.
3. Promote the availability of data for authorized users.

CONFIDENTIALITY



INTEGRITY

Figure 2. CIA Traid

1. Confidentiality:

Collecting, storing, and sharing data in the digital space have made us prone to cyber attacks. Confidentiality states that only authorized people should be able to access sensitive information.

Any Personal Identifiable Information (PII) that can help recognize a person, any financial information such as transaction details made on e-commerce sites is supposed to be kept confidential.

2. Integrity:

Ever remember clicking on a checkbox that says 'I declare that the information provided is correct and accurate to my knowledge? This is essentially a declaration of integrity.

Integrity maintains the dependability of information and ensures that it has been in its original form throughout and is exact. Stored data or data disseminated or used should not be altered at any time unless authorized by a licensed individual or system.

3. Availability:

Availability ensures the accessibility of information to authorized personnel at the right time. They should be able to process data whenever the need arises.

3.1.1. Definition and Importance of Cybersecurity

Definition

- Cyber Security is the technique of protecting your systems, digital devices, networks, and all of the data stored in the devices from cyber attacks. By acquiring knowledge of cyber attacks and cyber security we can secure and defend ourselves from various cyber attacks like phishing and DDoS attacks. It uses tools like firewalls and antivirus software to protect your devices from hackers and malware.

- Encryption is the technique that helps to keep your personal information private, you can only read it. Cybersecurity also teaches you how to spot tricks like phishing, where bad guys try to steal your info by pretending to be someone you trust. In short, cybersecurity keeps your online world safe and secure.

Importance of Cybersecurity

- Cybersecurity is essential for protecting our digital assets, including sensitive personal and financial information, intellectual property, and critical infrastructure. Cyberattacks can have serious consequences, including financial loss, reputational damage, and even physical harm.
- Cyber security is vital in any organization, no matter how big or small the organization is. Due to increasing technology and increasing software across various sectors like government, education, hospitals, etc., information is becoming digital through wireless communication networks. The importance of cyber security is to secure the data of various organizations like email, yahoo, etc., which have extremely sensitive information that can cause damage to both us and our reputation. Attackers target small and large companies and obtain their essential documents and information.
- Cybersecurity has become increasingly important in today’s interconnected world. As more and more data is stored and transmitted electronically, the risk of cyber-attacks has also increased. Cybersecurity is the practice of protecting computer systems, networks, and data from theft, damage, or unauthorized access.

3.1.2. Overview of Cybersecurity Principles and Goals

The overview of the cyber security principles is to provide strategic guidance on how an organization can protect their information technology and operational technology systems, applications and data from cyber threats. These cyber security principles are grouped into five functions:

1. GOVERN: Develop a strong cyber security culture.
2. IDENTIFY: Identify assets and associated security risks.
3. PROTECT: Implement controls to manage security risks.
4. DETECT: Detect and analyse cyber security events to identify cyber security incidents.
5. RESPOND: Respond to and recover from cyber security incidents

GOAL OF CYBERSECURITY

REDUCE THE RISK OF CYBER -ATTACKS

PROTECT ORGANIZATIONS, NETWORKS,TECHNOLOGIES

3.2. Threat Landscape and Cyber Security Trends

The threat landscape is the entirety of potential and identified cyberthreats affecting a particular sector, group of users, time period, and so forth.

3.2.1. Common and Cyber Emerging Threats

1. **Phishing:** This type of attack involves manipulating and tricking individuals into providing sensitive information, such as passwords or credit card numbers, through fake emails or websites. Phishing attacks have become common and more sophisticated, posing a significant threat to both individuals and businesses.
2. **Ransomware:** A major threat in recent years is ransomware, where criminals lock your files and demand a ransom amount to unlock them. These attacks have become more common and can target anyone from individuals to large organizations.
3. **Malware:** Malicious software, or malware, is designed to damage or disrupt computers and networks. It includes viruses, trojans, and spyware, and can be used to steal data, monitor user activity, or gain control of systems.
4. **Advanced Persistent Threats (APTs):** These are long-term targeted attacks often conducted by state-sponsored groups. APTs aim to steal data or disrupt operations over an extended period, often remaining undetected for months.
5. **IoT Vulnerabilities:** With more devices connected to the internet, like smart home gadgets and wearable devices, there are new opportunities for cyber attacks. Many of these devices lack strong security, which makies them easy targets for hackers.

6.Cloud Security: As more data is stored in the cloud, ensuring its security has become a top priority. Hackers are constantly trying to find ways to access this data, making cloud security a critical area of focus.

3.2.2. Impact of Cyber Threats

1. **Financial Loss:** Cyber threats can result in significant financial losses for individuals and organizations. Cybercriminals may steal sensitive financial information, conduct fraudulent transactions, or demand ransom payments to unlock encrypted data. The financial costs associated with investigating and mitigating cyber attacks, as well as potential legal liabilities and fines, can be substantial.
2. **Reputational Damage:** Cyber threats can cause reputational damage to individuals, businesses, and even governments. Data breaches and leaks of sensitive information can lead to a loss of trust among customers, partners, and the public. The negative publicity and damage to brand reputation can have long-term consequences, including loss of customers, partners, and business opportunities.
3. **Loss of Intellectual Property:** Cyber threats can result in the theft of intellectual property (IP), such as trade secrets, proprietary information, and research and development data.

This can significantly impact a company's competitive advantage and market position, leading to financial losses and loss of market share.

4. **Disruption of Operations:** Cyber attacks can disrupt critical operations of businesses and governments, causing downtime, loss of productivity, and delays in service delivery. For example, ransomware attacks can encrypt data and render systems or networks inaccessible, leading to business interruptions and financial losses.
5. **Legal and Regulatory Consequences:** Organizations may face legal and regulatory consequences as a result of cyber threats. Data protection and privacy laws, industry regulations, and contractual obligations may require organizations to implement certain security measures to protect sensitive information. Failure to comply with these requirements can result in legal penalties, fines, and lawsuits.
6. **National Security Risks:** Cyber threats can pose significant risks to national security. Cyber attacks targeting critical infrastructure, government systems, or military operations can disrupt essential services, compromise sensitive information, and impact national defense capabilities. This can have severe consequences on a country's security and sovereignty.
7. **Psychological and Emotional Consequences:** Cyber threats can also have psychological and emotional consequences for individuals. Victims of cyber attacks, such as identity theft or online harassment, may experience stress, anxiety, fear, and other negative emotions. These consequences can affect an individual's mental well-being and quality of life.

3.2.3. Cyber Security Trends and Importance of Threat Intelligence

Cyber Security Trends

1. **Rise of AI and Machine Learning:** More cybersecurity tools are using artificial intelligence (AI) and machine learning to detect and respond to threats faster than humans can. These technologies can analyse patterns and predict potential attacks, making them a valuable asset in protecting sensitive data.
2. **Increase in Ransomware Attacks:** Ransomware, where hackers lock you out of your data until you pay a ransom, is becoming more common. Companies and individuals alike need to back up their data regularly and invest in security measures to avoid falling victim to these attacks.
3. **Cloud Security:** As more businesses move their data to the cloud, ensuring this data is secure is a top priority. This includes using strong authentication methods and regularly updating security protocols to protect against breaches.
4. **Internet of Things (IoT) Vulnerabilities:** With more devices connected to the internet, like smart home gadgets and wearable tech, there's an increased risk of cyberattacks. Ensuring these devices have updated security features is crucial.
5. **Zero Trust Security:** This approach assumes that threats could come from inside or outside the network, so it constantly verifies and monitors all access requests. It's becoming a standard practice to ensure a higher level of security.

6. **Cybersecurity Skills Gap:** There is a growing need for skilled cybersecurity professionals. As cyber threats become more sophisticated, the demand for experts who can protect against these threats is higher than ever.

7. **Regulatory Compliance:** New regulations are being introduced worldwide to protect personal data. Companies must stay informed about these laws to ensure they comply and avoid hefty fines.

Importance of Threat Intelligence

1. **Protecting Sensitive Data.** With the increase in digitalization, data is becoming more and more valuable. Cybersecurity helps protect sensitive data such as personal information, financial data, and intellectual property from unauthorized access and theft.
2. **Prevention of Cyber Attacks.** Cyber attacks, such as Malware infections, Ransomware, Phishing, and Distributed Denial of Service (DDoS) attacks, can cause significant disruptions to businesses and individuals. Effective cybersecurity measures help prevent these attacks, reducing the risk of data breaches, financial losses, and operational disruptions.
3. **Safeguarding Critical Infrastructure.** Critical infrastructure, including power grids, transportation systems, healthcare systems, and communication networks, heavily relies on interconnected computer systems. Protecting these systems from cyber threats is crucial to ensure the smooth functioning of essential services and prevent potential disruptions that could impact public safety and national security.
4. **Maintaining Business Continuity.** Cyber attacks can cause significant disruption to businesses, resulting in lost revenue, damage to reputation, and in some cases, even shutting down the business. Cybersecurity helps ensure business continuity by preventing or minimizing the impact of cyber attacks.
5. **Compliance with Regulations.** Many industries are subject to strict regulations that require organizations to protect sensitive data. Failure to comply with these regulations can result in significant fines and legal action. Cybersecurity helps ensure compliance with regulations such as HIPAA, GDPR, and PCI DSS.
6. **Protecting National Security.** Cyber attacks can be used to compromise national security by targeting critical infrastructure, government systems, and military installations. Cybersecurity is critical for protecting national security and preventing cyber warfare.
7. **Preserving Privacy.** In an era where personal information is increasingly collected, stored, and shared digitally, cybersecurity is crucial for preserving privacy. Protecting personal data from unauthorized access, surveillance, and misuse helps maintain individuals' privacy rights and fosters trust in digital services.

3.3. Overview of Cybersecurity Framework and Standards

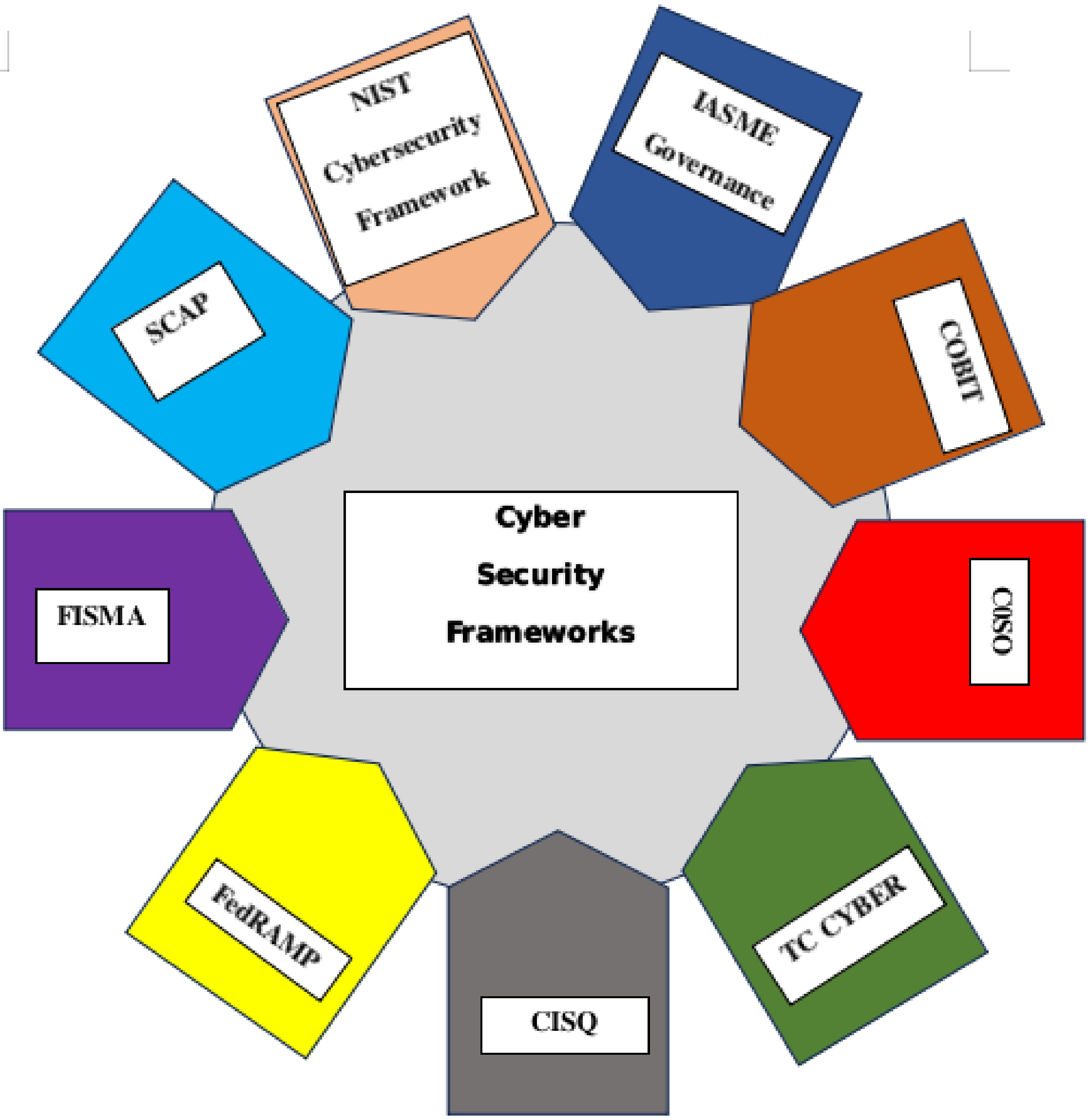


Figure 3. Cyber Security Frameworks

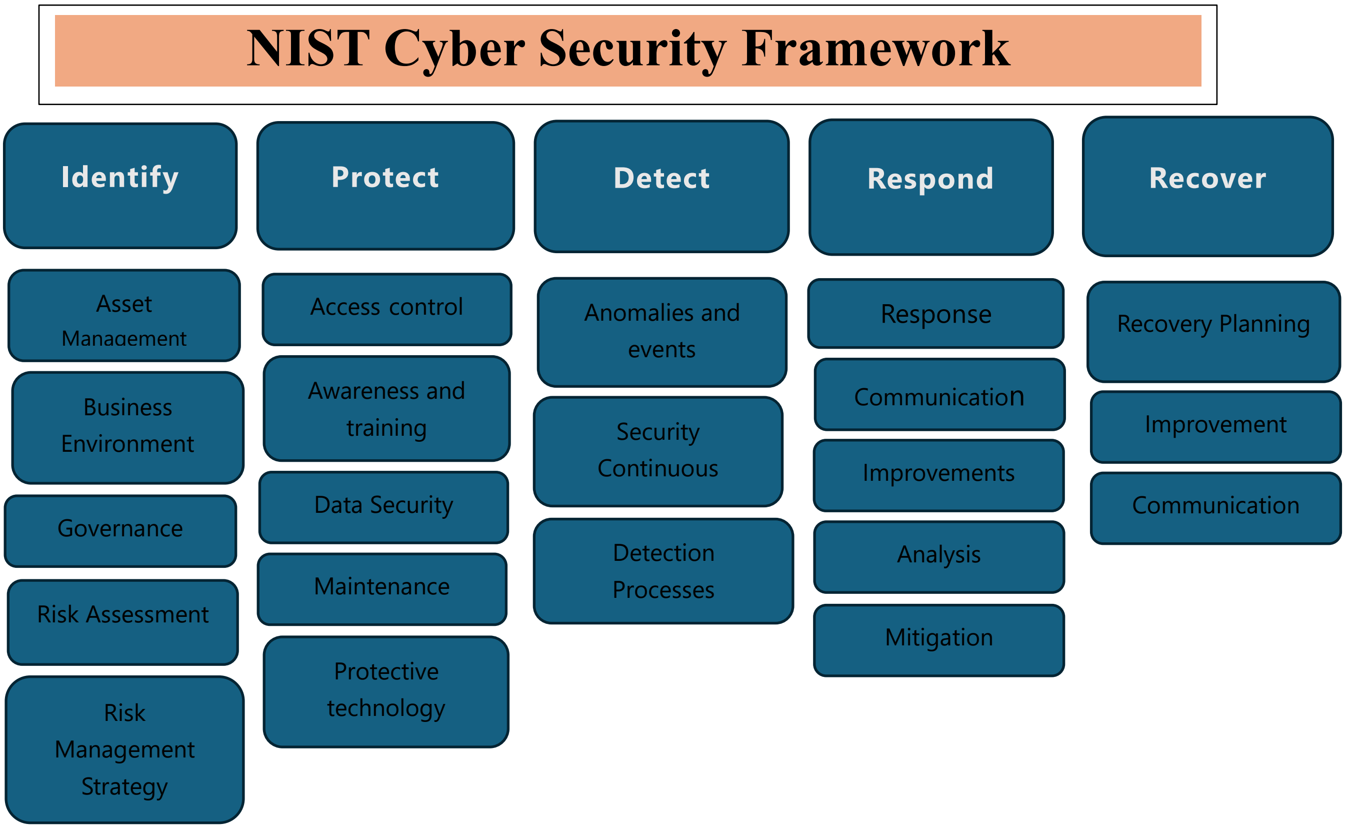
A cybersecurity framework is a structured set of guidelines and best practices designed to help organizations manage and mitigate cybersecurity risks associated with their information and technology systems. The goal of the framework is to reduce the company's exposure to cyberattacks, and to identify the areas most at risk for data breaches and other compromising activity perpetrated by cybercriminals. At its core, it provides a common language and systematic approach for ensuring an organization's digital assets, infrastructure, and data are adequately protected against cyber threats.

3.3.1. NIST Cybersecurity Framework

The National Institutes of Standards and Technology (NIST), a non-regulatory agency of the United States Department of Commerce, introduced the eponymously named NIST Cybersecurity framework in 2014. Initially designed for the benefit of private sector organizations in the United States, the NIST Cybersecurity framework is centered around five essential functions, namely:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

The NIST Cybersecurity Framework is one of the broadest frameworks provided by the NIST and applies to almost any organization seeking to build a cybersecurity program.



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access control	Anomalies and events	Response	Recovery Planning
Business Environment	Awareness and training	Security Continuous	Communication	Improvement
Governance	Data Security	Detection Processes	Improvements	Communication
Risk Assessment	Maintenance		Analysis	
Risk Management Strategy	Protective technology		Mitigation	

Figure 4. NIST Cyber Security Framework

3.3.2. COBIT Framework

COBIT (Control Objectives for Information and Related Technologies) is a framework created by the ISACA for IT management and governance. A highly process-oriented framework, COBIT's approach links business and IT goals together to delineate IT and Business teams' responsibilities.

COBIT identifies and advocates five processes: Evaluate, Direct and Monitor (EDM), Align, Plan and Organise (APO), Build, Acquire and Implement (BAI), Deliver, Service, and Support (DSS); Monitor, Evaluate and Assess (MEA).

COBIT was designed to cater to three objectives: legal compliance, increased agility, increased earning potential.

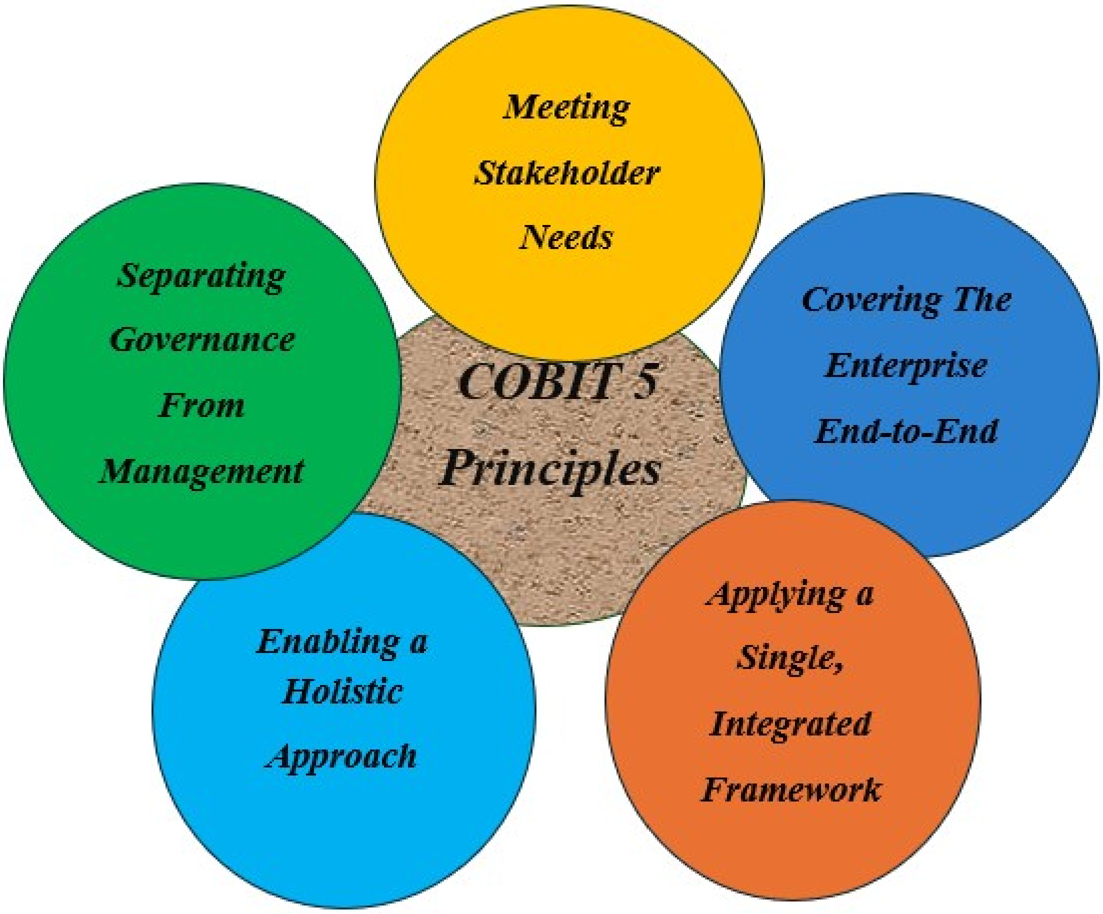

COBIT 5 Principles
Meeting Stakeholder Needs
Covering The Enterprise End-to-End
Applying a Single, Integrated Framework
Enabling a Holistic Approach
Separating Governance From Management

Figure 5. COBIT 5 Principles

3.3.3. GDPR and Data Protection Standards

The GDPR requires that personal data must be processed securely using appropriate technical and organisational measures. The Regulation does not mandate a specific set of cyber security measures but rather expects you to take 'appropriate' action. In other words you need to manage risk. What is appropriate for you will depend upon your circumstances as well as the data you are processing and therefore the risks posed, however there is an expectation you have minimal, established security measures in place. The security measures must be designed into your systems at the outset (referred to as Privacy by Design) and maintained effective throughout the life of your system.

Data protection is a core component of both cybersecurity and GDPR compliance.

The GDPR outlines six specific principles required of companies when processing personal data:

1. Lawfulness, fairness, and transparency
2. Purpose limitation

3. Data minimization
4. Storage limitation
5. Integrity and confidentiality
6. Overarching accountability

Data protection is the process of protecting sensitive information from damage, loss, or corruption.

Most data protection strategies have three key focuses:

- **Data security** – protecting data from malicious or accidental damage
- **Data availability –** Quickly restoring data in the event of damage or loss

Access control – ensuring that data is accessible to those who actually need it, and not to anyone else

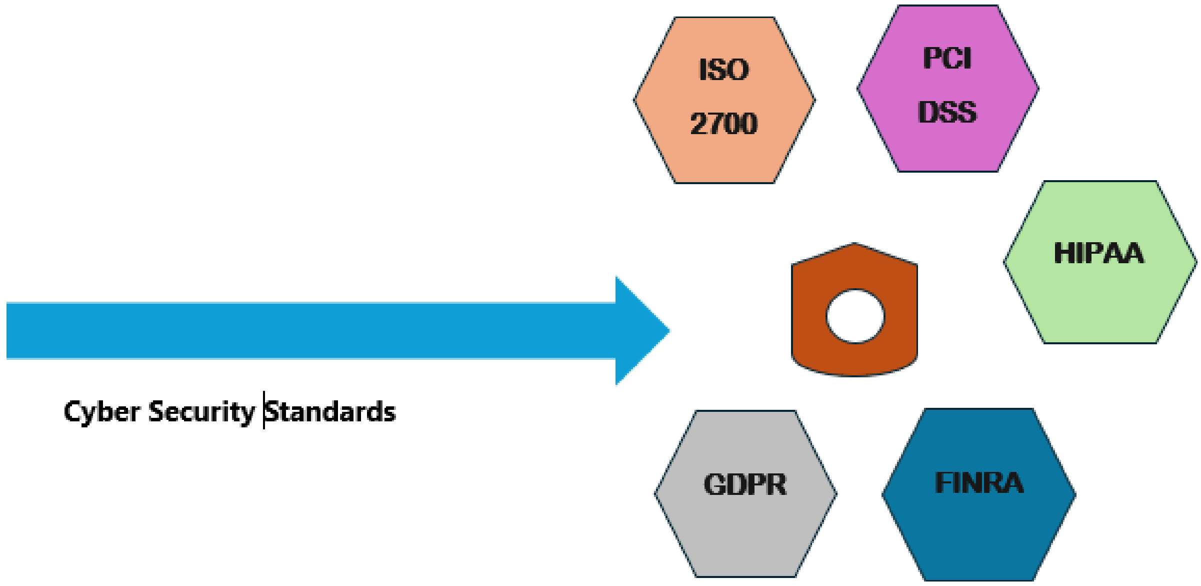


Figure 6. Cyber Security standards

Cyber Security standard may be defined as the set of rules that an organization has to comply in order to gain right for some particular things like for accepting online payment, for storing patient data and so on. The standards consist of some of the basic rules that the organization is supposed to obey in order to maintain compliance with any of the cybersecurity standards.

Below are some of the common and important standards:

1. **ISO 27001**. This is one of the common standards that adhere to the organization to implement an Information security management system. It is comprised of the set of procedures that states the rules and requirements which has to be satisfied in order to get the organization certified with this standard. As per this standard, the organization is supposed to keep all the technology up to date, the servers should exist without vulnerabilities and the organization has to be audited after the specified interval to remain compiled to this standard. It is an international standard and every organization that serves other organization that complies with this standard is supposed to comply with ISMS policy that is covered under ISO 27001 practice.

2. **PCI DSS.** PCI DSS stands for Payment Card Industry Data Security Standard. This can be considered as the standard that has to be opted by the organization that accepts payment through their gateway. The businesses that store user data like their name and card related information must have to adopt this standard in their organization. As per this compliance, the technologies used by the organization should be up-to-date and their system should continuously undergo the security assessment to ensure that it is not having any severe vulnerability. This standard was developed by the cluster of card brands (American Express, Visa, MasterCard, JCB, and Discover).
3. **HIPAA.** HIPAA stands for Health Insurance Portability and Accountability Act. It is the standard that the hospitals are supposed to follow to ensure that their patient's data are fully protected and cannot be leaked anyway. In order to comply with this standard, the hospital must have a strong network security team who takes care of all the security incidents, their quarterly security reports should be healthy, all the transaction has to be done in encrypted mode and so on. This standard ensures that the critical health-related information of the patient will remain secure so that the patient can feel safe about their health.
4. **FINRA.** FINRA stands for Financial Industry Regulatory Authority. This standard is all about making things secure for the financial bodies that handle the funds or aggressively engaged in financial transactions. In this standard, the system is supposed to be highly secure and to comply with this standard, various measures have to be considered in terms of data security and the user's data protection. It is one of the most essential standards that all the organizations based on finance are supposed to comply with.
5. **GDPR.** GDPR stands for General Data Protection Regulation. It is a standard defined by the European government which is concerned about the data protection of all the users. In this standard, the body that has to manage the compliance has to make sure that the user's data is secure and cannot be accessed without proper authorization. As the name states, this standard mainly focuses on the safety of the user's data so that they can feel safe while sharing it with any of the organizations that are complying with the General Data Protection Regulation.

3.3.4. Implementing Cybersecurity Framework

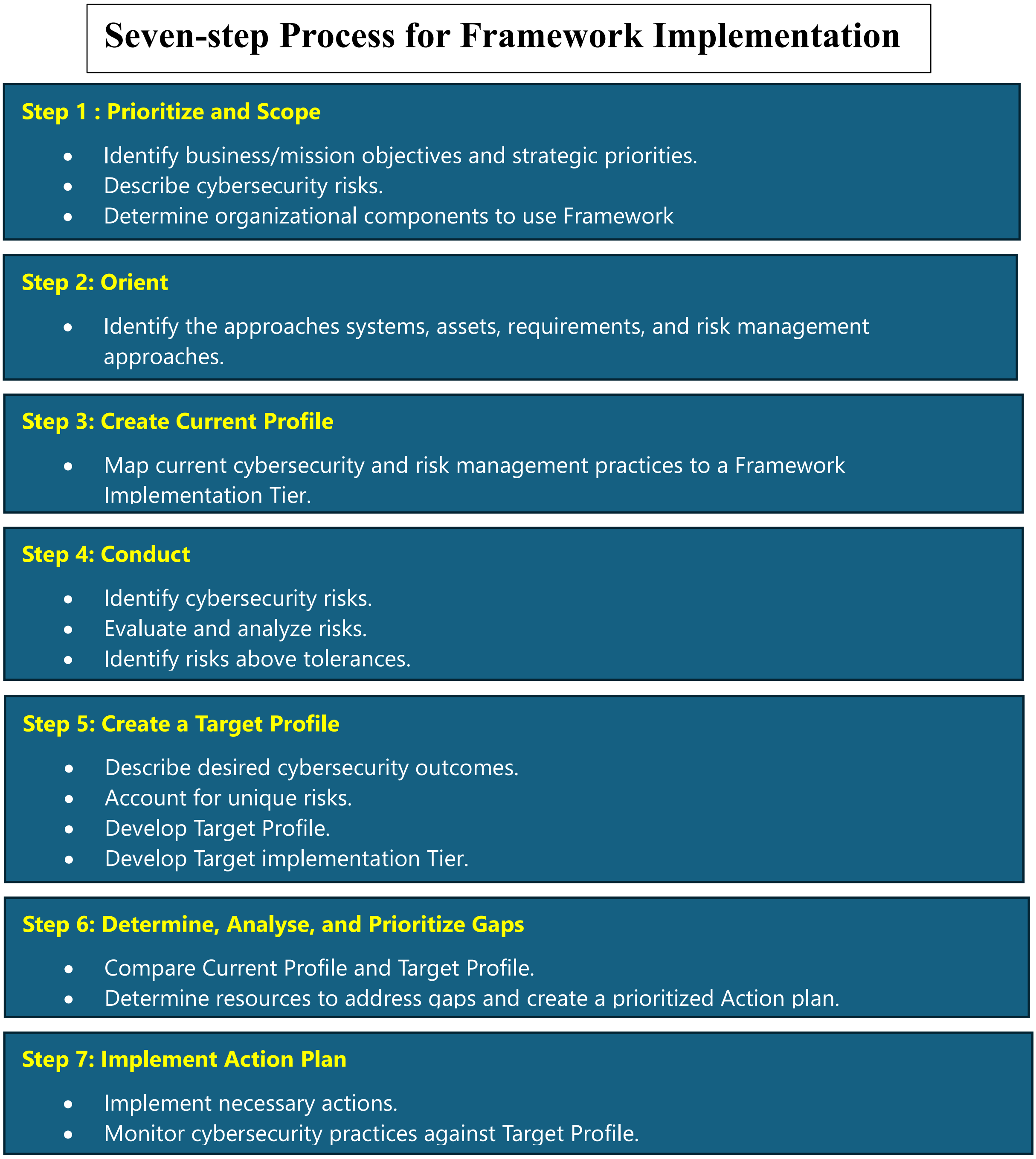
The Framework can be applied through a seven-step process, shown below in Figure Seven-step Process for Framework Implementation

Step 1: Prioritize and Scope

When implementing the Framework, an organization first identifies its business or mission objectives and its strategic priorities as they relate to cybersecurity. With this information, an organization can make decisions regarding cybersecurity implementation and determine the breadth and scope of systems and assets that support its objectives. An organization can adapt the Framework to support different business lines or processes, which may have different business needs and associated risk tolerance.

Step 2: Orient

At this stage, an organization identifies the systems, assets, requirements, and risk management approaches that fall within the scope of the effort. This includes current organization standards and best practices, as well as any additional items that can enable the organization to achieve its critical infrastructure and business objectives for cybersecurity risk management. The organization's risk management program may have already identified and documented much of this information. In general, organizations should focus initially on critical systems and assets and then expand into systems and assets that are less critical or central to their mission.



Seven-step Process for Framework Implementation

Step 1 : Prioritize and Scope

- Identify business/mission objectives and strategic priorities.
- Describe cybersecurity risks.
- Determine organizational components to use Framework

Step 2: Orient

- Identify the approaches systems, assets, requirements, and risk management approaches.

Step 3: Create Current Profile

- Map current cybersecurity and risk management practices to a Framework Implementation Tier.

Step 4: Conduct

- Identify cybersecurity risks.
- Evaluate and analyze risks.
- Identify risks above tolerances.

Step 5: Create a Target Profile

- Describe desired cybersecurity outcomes.
- Account for unique risks.
- Develop Target Profile.
- Develop Target implementation Tier.

Step 6: Determine, Analyse, and Prioritize Gaps

- Compare Current Profile and Target Profile.
- Determine resources to address gaps and create a prioritized Action plan.

Step 7: Implement Action Plan

- Implement necessary actions.
- Monitor cybersecurity practices against Target Profile.

Figure 7. Seven-step Process for Framework Implementation

Step 3: Create a Current Profile

The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. The purpose of identifying a Current Profile is not only to develop a map between organizational practices and Category and Subcategory outcomes, but also to help understand the extent to which such practices achieve the outcomes outlined by the Framework.

Step 4: Conduct a Risk Assessment

This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyses the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that the organization incorporates emerging risk, threat, and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events. The results of cybersecurity risk assessment activities allow the organization to develop its Target Profile and identify a Target Implementation Tier, which occurs in Step 5. For organizations that already have a risk management program in place, this activity will be part of regular business practice, and necessary records and information to make this determination may already exist

Step 5: Create a Target Profile

In creating a Target Profile, organizations should consider:

- current risk management practices,
- current risk environment,
- legal and regulatory requirements,
- business and mission objectives, and
- organizational constraints.

The Target Profile outlines the key Category and Subcategory outcomes and associated cybersecurity and risk management standards, tools, methods, and guidelines that will protect against cybersecurity risks in proportion to the risks facing organizational and critical infrastructure security objectives. As highlighted in Step 3, the Framework gives organizations a broad overview of the cybersecurity and risk management domains, but it is not all-inclusive.

Step 6: Determine, Analyze, and Prioritize Gaps

The organization compares the Current Profile and the Target Profile to determine gaps. To address those gaps, it creates a prioritized action plan that draws on mission drivers, a cost/benefit analysis, and an understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and allows the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan

The organization determines which actions to take regarding the gaps (if any) identified in the previous step, and then monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies Informative References regarding the

Categories and Subcategories. Organizations should determine which standards, guidelines, and practices, including those that are sector-specific, work best for their needs.

Reference Books:

1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
2. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.
3. Cyber SecurityEssentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
4. Introduction to Cyber Security,Chwan-Hwa(john) Wu,J.David Irwin.CRC PressT&FGroup

Reference Links:

1. https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Security
2. https://academic.oup.com/cybersecurity
3. https://www.sciencedirect.com/science/article/pii/S2352484721007289
4. https://www.techscience.com/journal/JCS

Question Answers

Q.No. 01 **Marks**

Question: How do firewalls protect network security? **05**

Answer: Firewalls protect network security by acting as a barrier between trusted internal networks and untrusted external networks, such as the internet. Here's how they do it:

1. **Traffic Filtering**: Firewalls analyze incoming and outgoing traffic based on predefined security rules.
2. **Stateful Inspection**: Many modern firewalls perform stateful inspection, which tracks the state of active connections and makes decisions based on the context of the traffic, rather than just static rules.
3. **Access Control**: Firewalls enforce access control policies, ensuring that only authorized users and devices can access certain resources within the network.

Q. No.02 **05**

Question: What steps would you take if you discovered a security breach?

Answer:

1. Assess the Situation
2. Contain the Breach
3. Notify Relevant Stakeholders
4. Investigate
5. Remediate Vulnerabilities
6. Communicate Externally
7. Review and Improve Security Measures
8. Document Everything
9. Monitor for Further Issues

Q. No.03 **05**

Question: Elaborate the common cyber threats today?

Answer: Phishing: Fraudulent attempts to obtain sensitive information (like usernames and passwords) by masquerading as trustworthy entities, often through emails or fake websites.

Ransomware: Malicious software that encrypts a victim's files, demanding a ransom for the decryption key. This can lead to significant data loss and operational disruption.

Malware: Any software designed to harm or exploit devices and networks. This includes viruses, worms, Trojans, and spyware.

Q. No.04 **05**

Question: Elaborate the concept of risk assessment in cybersecurity.

Answer: Risk assessment in cybersecurity is the process of identifying, evaluating, and prioritizing risks to an organization’s information assets and systems.
Risk assessment in cybersecurity is a crucial process that helps organizations identify, evaluate, and prioritize potential risks to their information systems.

Q. No.05 **05**

Question: Discuss the role of artificial intelligence in cybersecurity.

Answer: Artificial intelligence (AI) plays a significant role in enhancing cybersecurity by automating processes, improving threat detection, and enabling more effective response strategies. Here are some key areas where AI is making an impact:

1. Threat Detection and Prevention
2. Incident Response
3. Behavioral Analysis
4. Predictive Analytics
5. Automating Security Operations
6. Enhanced Security Analytics
7. Fraud Detection

Q. No.06 **05**

Question: Discuss the role of artificial intelligence in cybersecurity.

Answer: Artificial intelligence (AI) plays a significant role in enhancing cybersecurity by automating processes, improving threat detection, and enabling more effective response strategies. Here are some key areas where AI is making an impact:

1. Threat Detection and Prevention
2. Incident Response
3. Behavioral Analysis
4. Predictive Analytics
5. Automating Security Operations
6. Enhanced Security Analytics
7. Fraud Detection
8.

Q. No.07 **05**

Question: Explain the critical components of NIST Cybersecurity framework?

Answer: The NIST Cybersecurity Framework (CSF) is a comprehensive guide designed to help organizations manage and reduce cybersecurity risk.
Identify: Understanding the organization's environment, including assets, risks, and regulatory requirements, to inform cybersecurity risk management.
Protect: Implementing safeguards to ensure the delivery of critical services. This includes access controls, awareness training, data security, and protective technologies.

Q. No.08 **05**

Question: Discuss the critical components of NIST Cybersecurity framework?

Answer: The NIST Cybersecurity Framework (CSF) is a comprehensive guide designed to help organizations manage and reduce cybersecurity risk.
Identify: Understanding the organization's environment, including assets, risks, and regulatory requirements, to inform cybersecurity risk management.
Protect: Implementing safeguards to ensure the delivery of critical services. This includes access controls, awareness training, data security, and protective technologies.
Detect: Developing and implementing activities to identify the occurrence of a cybersecurity event. This includes continuous monitoring and anomaly detection.
Respond: Planning and implementing appropriate actions in response to detected cybersecurity incidents. This involves response planning, communications, and analysis.
Recover: Ensuring the organization can recover from cybersecurity incidents and maintain resilience. This includes recovery planning and improvements based on lessons learned.

Q. No.09 **05**

Question:Difference between "Threat Intelligence" and "Security Intelligence."

Answer:Threat intelligence refers to the information and insights about potential or existing threats to an organization's assets, including data, systems, and networks. It includes data about threat actors, attack methods, vulnerabilities, and indicators of compromise (IoCs).

Security intelligence encompasses the broader analysis and interpretation of security-related data within an organization. It includes insights derived from various security tools, logs, and events across the organization's infrastructure.

Q. No.10 **05**

Question: Elaborate on the history of COBIT

Answer:COBIT was released by ISACA in the year of 1996. It was formed with an objective to maneuver the financial audit of the IT-related workforce. Expanding it further than just auditing a better version was released in the year of 1998. And the third version with the guidelines for management was released in the year 2000. The later versions of 4 were released in 2005 and the 4.1 was released in the year 2007.

Q. No.11 **05**

Question: How does Brexit affect GDPR?

Answer: If a company processes data about individuals in the context of selling goods or services to citizens in other EU countries, it needs to comply with the GDPR.

From the 1st of January 2021, the UK stopped being part of the EU, meaning that the EU GDPR no longer protected UK citizens. Now, the general data protection regime that applies to most UK businesses and organisations is the UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018. It explains each of the data protection principles, rights and obligations. It summarises the key points you need to know, answers frequently asked questions and contains practical checklists to help you comply.