ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Cyber Law, Policy and Compliance

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Introduction

This presentation covers major Standards concerning Cyber Security, dealing with applicable regulations, standards, laws and certifications that are relevant to any kind of Company, focusing, where applicable, on Small and Medium Enterprises (SMEs).

The **ISO/IEC 27000** family of standards is a series of best practices that aims helping organizations improve their information security.

General Data Protection Regulation (GDPR) is a law made by EU mainly to protect data privacy and that is quite important for all sizes of companies.

Control Objectives for Information and Related Technology (COBIT) is a framework for IT governance and management.

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Introduction

The IT Infrastructure Library (ITIL) aims to improve controls for service management.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a framework that provides set of guidelines on enterprise risk management, internal control and fraud deterrence.

Network and Information Security (NIS) guidelines are finalized to enhance cybersecurity across the EU.

Finally, an overview on **IT security Certifications (for individuals)** is provided: professionals with a strong background in IT Security are more and more needed nowadays.

Back to Index

ENGINE

Co-funded by the Erasmus+ Programme of the European Union

Index

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

ISO 27000 series Standards

The ISO/IEC 270001 family of standards is a series of best practices that aim at helping organizations improve their information security.

Published by ISO (the International Organization for Standardization) and the IEC (International Electrotechnical Commission), the series explains how to implement best-practice information security practices: **ISMS (information security management system)** requirements are described.

An ISMS is a systematic approach to risk management, containing measures that address the three pillars of information security: **people, processes and technology.**

The series consists of 46 individual standards; there is no need to know all of them, also considering that some won't be relevant to your organization, but there are a few core ones that, in general, SMEs should be familiar with and that will be covered in this document.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

ISO 27000 series Standards

- ISO 27001
  - It is the major standard in the ISO 27000 series, as it contains the implementation requirements for an ISMS.
  - ISO IEC 27001: 2013 is the only standard in the series that organisations c**an be audited and certified against**.
- ISO 27002
  - This is a supplementary standard that provides an overview of information security controls that organisations might choose to implement
- ISO/IEC 27005:2018
  - ISO 27005 provides guidance for information security risk management in line with ISO 27001, helping organisations take a risk-based approach to information security.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

ISO 27000 series Standards

- ISO 27017 and ISO 27018
  - These supplementary ISO standards were introduced in 2015, explaining how organisations should protect sensitive information in the Cloud.

- ISO 27701
  - This is the newest standard in the ISO 27000 series, covering what organisations must do when implementing a PIMS (Privacy Information Management System).

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

ISO/IEC 27001:2013

ISO/IEC 27001:2013 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS

ISO/IEC 27001:2013 has ten short clauses, plus a long annex, which cover:

- 1. Scope of the standard
- 2. How the document is referenced
- 3. Reuse of the terms and definitions in ISO/IEC 27000
- 4. Organizational context and stakeholders
- 5. Information security leadership and high-level support for policy
- 6. Planning an information security management system; risk assessment; risk treatment
- 7. Supporting an information security management system
- 8. Making an information security management system operational
- 9. Reviewing the system's performance
- 10. Corrective action
- **Annex A: List of controls and their objectives**

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

ISO/IEC 27001:2013

Annex A of ISO 27001 is probably the most famous annex of all the ISO standards – this is because it provides an essential tool for managing information security risks: a list of security controls (or safeguards) that are to be used to improve the security of information assets.

The ISO 27001 controls list can be found in Annex A, and it is organized into 14 sections (domains).

Here's a short description of each of the 14 sections:

- A.5 Information security policies – controls on how the policies are written and reviewed
- A.6 Organization of information security – controls on how the responsibilities are assigned; also includes the controls for mobile devices and teleworking
- A.7 Human resources security – controls prior to employment, during, and after the employment

Back to Index

ENGINE

Co-funded by the Erasmus+ Programme of the European Union

ISO/IEC 27001:2013

- A.8 Asset management – controls related to inventory of assets and acceptable use; also for information classification and media handling
- A.9 Access control – controls for the management of access rights of users, systems and applications, and for the management of user responsibilities
- A.10 Cryptography – controls related to encryption and key management
- A.11 Physical and environmental security – controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, Clear Desk and Clear Screen Policy, etc.
- A.12 Operational security – lots of controls related to the management of IT production: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, etc.
- A.13 Communications security – controls related to network security, segregation, network services, transfer of information, messaging, etc.

Back to Index

ENGINE

Co-funded by the Erasmus+ Programme of the European Union

ISO/IEC 27001:2013

- A.14 System acquisition, development and maintenance – controls defining security requirements, and security in development and support processes
- A.15 Supplier relationships – controls on what to include in agreements, and how to monitor the suppliers
- A.16 Information security incident management – controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence
- A.17 Information security aspects of business continuity management – controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy
- A.18 Compliance – controls requiring the identification of applicable laws and regulations, intellectual property protection, personal data protection, and reviews of information security

NOTE: Not all of these ISO 27001:2013 controls are mandatory – **organizations can choose for themselves which controls they find applicable, and then they must implement them** (in most cases, at least 90% of the controls are applicable); the rest are declared to be inapplicable.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

ISO/IEC 27002

ISO/IEC 27002:2013 INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS

- ISO/IEC 27002 is a popular, internationally-recognized standard of good practice for information security.
- The Information Security Management System formally defined by ISO/IEC 27001 uses a summary of ISO/IEC 27002 in Annex A to suggest potential information security controls worth considering. However, organizations are free to select and implement other controls as they see fit. In practice, most organizations that adopt ISO/IEC 27001 also use ISO/IEC 27002 as a framework or starting point for their controls, making various changes as necessary to suit their information risk treatment requirements.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

ISO/IEC 27005

ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management

- The standard ‘provides guidelines for information security risk management’ and ‘supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.’
- The standard doesn't specify, recommend or even name any specific risk management method. However, it implies a continual process consisting of a structured sequence of activities, some of which are iterative.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

ISO/IEC 27017

ISO/IEC 27017:2015 / ITU-T X.1631 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

- This standard provides guidance on the information security aspects of cloud computing, recommending and assisting with the implementation of cloud-specific information security controls supplementing the guidance in ISO/IEC 27002 and other ISO27k standards.
- The code of practice provides additional information security controls implementation advice beyond that provided in ISO/IEC 27002, in the cloud computing context.
- The standard advises both cloud service customers and cloud service providers with the primary guidance laid out side-by-side in each section. For instance, section 6.1.1 on information security roles and responsibilities says, in addition to section 6.1.1 of ISO/IEC 27002:2013:

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

ISO/IEC 27017

- The standard advises both cloud service customers and cloud service providers with the primary guidance laid out side-by-side in each section. For instance, section 6.1.1 on information security roles and responsibilities says, in addition to section 6.1.1 of ISO/IEC 27002:2013:

Cloud service customer	Cloud service provider
The cloud service customer should agree with the cloud service provider on an appropriate allocation of information security roles and responsibilities, and confirm that it can fulfil its allocated roles and responsibilities. The information security roles and responsibilities of both parties should be stated in an agreement. The cloud service customer should identify and manage its relationship with the customer support and care function of the cloud service provider.	The cloud service provider should agree and document an appropriate allocation of information security roles and responsibilities with its cloud service customers, its cloud service providers, and its suppliers.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

ISO/IEC 27018

ISO/IEC 27018:2019 — Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors

- The standard intends to be “a reference for selecting PII protection controls within the process of implementing a cloud computing information security management system based on ISO/IEC 27001, or as a guidance document for organizations for implementing commonly accepted PII protection controls”
- The standard is primarily concerned with public-cloud computing service providers acting as PII processors . “A public cloud service provider is a 'PII processor' when it processes PII for and according to the instructions of a cloud service customer”.

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

ISO/IEC 27018

Let's see first to what degree ISO 27018 suggests that existing controls should be augmented:

ISO 27001/ISO 27002 controls additions to ISO 27018	
ISO 27001/ISO 27002 control section	**Level of additional items in ISO 27018**
5 Information security policies	Moderate
6 Organization of information security	Low
7 Human resource security	Low
8 Asset management	Low
9 Access control	Low
10 Cryptography	Low
11 Physical and environmental security	Low
12 Operations security	High
13 Communications security	Low
14 System acquisition, development and maintenance	Low
15 Supplier relationships	Low
16 Information security incident management	Moderate
17 Information security aspects of business continuity management	Low
18 Compliance	Moderate

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

ISO/IEC 27018

Annex A of ISO 27018 lists the following additional controls (that do not exist in ISO 27001/27002) that should be implemented in order to increase the level of protection of personal data in the cloud:

- Rights of the customer to access and delete the data; Processing the data only for the purpose for which the customer has provided it
- Not using the data for marketing and advertising; Deletion of temporary files
- Notification to the customer in case of a request for data disclosure; recording all the disclosures of personal data
- Disclosing the information about all the sub-contractors used for processing the personal data
- Notification to the customer in case of a data breach; Document management for cloud policies and procedures;policy for return, transfer and disposal of personal data
- Confidentiality agreements for individuals who can access personal data

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

ISO/IEC 27018

- Restriction of printing the personal data; Procedure for data restoration
- Authorization for taking the physical media off-site
- Restriction of usage of media that does not have encryption capability; encrypting data that is transmitted over public networks
- Destruction of printed media with personal data; usage of unique IDs for cloud customers; records of user access to the cloud; disabling the usage of expired user IDs
- Specifying the minimum security controls in contracts with customers and subcontractors
- Deletion of data in storage assigned to other customers
- Disclosing to the cloud customer in which countries the data will be stored
- Ensuring the data reaches the destination

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

ISO/IEC 27701

ISO/IEC 27701:2019 — Information technology — Security techniques — Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy information management

The UK DPA (Data Protection Act) 2018, the UK GDPR (General Data Protection Regulation), and the EU GDPR (General Data Protection Regulation) require organisations to take measures to ensure the privacy of any personal data that they process.

However, none of these laws provides much guidance on how those measures should look like.

The ISO (the International Organization for Standardization) and the IEC (International Electrotechnical Commission) developed this new standard to provide that guidance.

ISO/IEC 27701 (*Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*), published in August 2019, aims to fill the assurance gap and provide a genuinely international approach to data protection as an extension of information security.

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

ISO/IEC 27701

How can ISO/IEC 27701 be used to comply with GDPR?

Implementing a management system compliant with ISO/IEC 27701 and ISO/IEC 27001 will enable your company to meet the privacy and information security requirements set forth in GDPR as well as other data protection regulations. GDPR requires organizations to adopt appropriate technical and organizational measures (including policies, procedures and processes) to protect the personal data they process.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a Law about privacy; it was drafted and passed by the European Union (EU) and it imposes obligations onto organizations anywhere, when they target or collect **data related to natural persons**. The regulation has been applied since May 25, 2018.

The GDPR defines an array of legal terms at length. Below are some of the most important ones that we refer to in this article:

- Personal data — Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. Pseudonymous data can also fall under the definition if it's relatively easy to ID someone from it.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

General Data Protection Regulation (GDPR)

- Data processing — Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing... so basically anything.
- Data subject — The person whose data is processed. These are your customers or site visitors.
- Data controller — The person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you.
- Data processor — A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations. They could include cloud servers or email service providers.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

General Data Protection Regulation (GDPR)

- Data protection principles - if you process data, you have to do so according to seven protection and accountability principles outlined in Article 5.1-2:

1. Lawfulness, fairness and transparency — Processing must be lawful, fair, and transparent to the data subject.
2. Purpose limitation — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. Data minimization — You should collect and process only as much data as absolutely necessary for the purposes specified.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

General Data Protection Regulation (GDPR)

4. Accuracy — You must keep personal data accurate and up to date.
5. Storage limitation — You may only store personally identifying data for as long as necessary for the specified purpose.
6. Integrity and confidentiality — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7. Accountability — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

General Data Protection Regulation (GDPR)

Accountability

The GDPR says data controllers have to be able to demonstrate they are GDPR compliant. And this isn't something you can do after the fact: If you think you are compliant with the GDPR but can't show how, then you're not GDPR compliant.

How can you show that you are GDPR compliant: = flashcard

- Designate data protection responsibilities to your team.
- Maintain detailed documentation of the data you're collecting, how it's used, where it's stored, which employee is responsible for it, etc.
- Train your staff and implement technical and organizational security measures.
- Have Data Processing Agreement contracts in place with third parties you contract to process data for you.
- Appoint a Data Protection Officer (though not all organizations need one see on

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

General Data Protection Regulation (GDPR)

Data security

You're required to handle data securely by implementing "appropriate technical and organizational measures." Technical measures mean anything from requiring your employees to use two-factor authentication on accounts where personal data are stored to contracting with cloud providers that use end-to-end encryption.

Organizational measures are things like staff trainings, adding a data privacy policy to your employee handbook, or limiting access to personal data to only those employees in your organization who need it.

If you have a data breach, you have 72 hours to tell the data subjects otherwise you face penalties. (This notification requirement may be waived if you use technological safeguards, such as encryption, to render data useless to an attacker.)

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

General Data Protection Regulation (GDPR)

Data protection by design and by default

From now on, everything you do in your organization must, “by design and by default,” consider data protection. Practically speaking, this means you must consider the data protection principles in the design of any new product or activity.

For example: you are launching a new app for your company. You have to think about what personal data the app could possibly collect from users, then consider ways to minimize the amount of data and how you will secure it with the latest technology.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

General Data Protection Regulation (GDPR)

When you're allowed to process data = flashcard

Article 6 lists the instances in which it's legal to process person data. Don't even think about touching somebody's personal data — don't collect it, don't store it, don't sell it to advertisers — unless you can justify it with one of the following:

- The data subject gave you specific, unambiguous consent to process the data. (e.g. They've opted in to your marketing email list.)
- Processing is necessary to execute or to prepare to enter into a contract to which the data subject is a party. (e.g. You need to do a background check before leasing property to a prospective tenant.)
- You need to process it to comply with a legal obligation of yours. (e.g. You receive an order from the court in your jurisdiction.)
- You need to process the data to save somebody's life. (e.g. Well, you'll probably know when this one applies.) = back of the flashcard

back to index

Co-funded by the
Erasmus+ Programme
of the European Union

General Data Protection Regulation (GDPR)

- Processing is necessary to perform a task in the public interest or to carry out some official function. (e.g. You're a private garbage collection company.)
- You have a legitimate interest to process someone's personal data. This is the most flexible lawful basis, though the "fundamental rights and freedoms of the data subject" always override your interests, especially if it's a child's data. (It's difficult to give an example here because there are a variety of factors you'll need to consider for your case. The UK Information Commissioner's Office provides helpful guidance here.) = back of the previous falshcard

Once you've determined the lawful basis for your data processing, you need to document this basis and notify the data subject (transparency!). And if you decide later to change your justification, you need to have a good reason, document this reason, and notify the data subject.

Back to Index

ENGINE

Co-funded by the Erasmus+ Programme of the European Union

General Data Protection Regulation (GDPR)

Consent

There are strict new rules about what constitutes consent from a data subject to process their information. = falshcard

- Consent must be “freely given, specific, informed and unambiguous.”
- Requests for consent must be “clearly distinguishable from the other matters” and presented in “clear and plain language.”
- Data subjects can withdraw previously given consent whenever they want, and you have to honor their decision. You can’t simply change the legal basis of the processing to one of the other justifications.
- Children under 13 can only give consent with permission from their parent.
- You need to keep documentary evidence of consent. = back of the flashcard

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

General Data Protection Regulation (GDPR)

Data Protection Officers

Contrary to popular belief, not every data controller or processor needs to appoint a Data Protection Officer (DPO). There are three conditions under which you are required to appoint a DPO:

- You are a public authority other than a court acting in a judicial capacity.
- Your core activities require you to monitor people systematically and regularly on a large scale. (e.g. You're Google.)
- Your core activities are large-scale processing of special categories of data listed under Article 9 of the GDPR or data relating to criminal convictions and offenses mentioned in Article 10. (e.g. You're a medical office.)

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Does GDPR applie to SMEs?

Does GDPR affect Small and Medium Enterprises? The answer is yes.

The application of the data protection regulation depends not on the size of your company/organisation but on the nature of your activities. Activities that present high risks for the individuals' rights and freedoms, whether they are carried out by an SME or by a large corporation, trigger the application of more stringent rules. However, some of the obligations of the GDPR may not apply to all SMEs.

For instance, **companies with fewer than 250 employees don't need to keep records of their processing activities unless processing of personal data is a regular activity**, **poses a threat to individuals' rights and freedoms, or concerns sensitive data or criminal records.**

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Does GDPR applies to SMEs?

Similarly, SMEs will only have to appoint a Data Protection Officer if processing is their main business and it poses specific threats to the individuals' rights and freedoms (such as monitoring of individuals or processing of sensitive data or criminal records) in particular because it's done on a large scale.

When the GDPR came into effect, there was a misconception that it only applied to multinationals, and that small business owners didn't need to bother with it.

The truth is that the Regulation applies to all organisations that process EU residents' personal data, whether they are sole traders, small businesses or conglomerates.

Note: even a Company with only one employee has to comply with GDPR, as it is managing employee's personal data.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

GDPR: what to do (in practice?)

Protect the rights of people giving you their data:

Communication:

Use plain language. Tell them who you are when you request the data. Say why you are processing their data, how long it will be stored and who receives it.

Consent:

Consent is one of the legal grounds for processing data (together with contract, legitimate interest, legal obligations, etc.). If you rely on it, consent should be given by a clear affirmative action.

Access and portability:

Let people access their data and give it to another company.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

GDPR: what to do (in practice?)

Warnings:

Inform people of data breaches if there is a serious risk to them

Erase data

Give people the 'right to be forgotten'. Erase their personal data if they ask, but only if it doesn't compromise freedom of expression or the ability to research.

Profiling

If you use profiling to process applications for legally-binding agreements like loans you must:

- Inform your customers; Make sure you have a person, not a machine, checking the process if the application ends in a refusal; Offer the applicant the right to contest the decision; Ensure an appropriate legal basis to carry out such profiling.

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

GDPR: what to do (in practice?)

Marketing:

Give people the right to opt out of direct marketing that uses their data.

Safeguarding sensitive data

Use extra safeguards for information on **health, race, sexual orientation, religion and political beliefs.**

Children's data

Collecting data from children under 16? Under the GDPR you must get parental consent. However, each EU Member State can lower this threshold to between 13 and 16 years of age, so check the age limit.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

GDPR: what to do (in practice?)

Data Transfer outside the EU

Check availability of transfer tool like model contract clauses when there is no adequacy decision for the country of destination.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

GDPR: what to do (in practice?)

Check if you need a Data Protection Officer (DPO)

As mentioned before, that is not always mandatory. It depends on the type and amount of data you collect, whether processing is your main business and if you do it on a large scale.

Some examples:

- You process personal data to target advertising through search engines based on people's behaviour online: Yes
- You send your clients an advert once a year to promote your local food business: No
- You are a GP and collect data on your patients' health: No
- You process personal data on genetics and health for a hospital: Yes

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

GDPR: what to do (in practice?)

Keep records

You should keep records of data processing containing:

- Name and contact details of business
- Reasons for data processing
- Description of categories of data subjects and personal data
- Categories of organisations receiving the data
- Transfer of data to another country or organisation
- Time limit for removal of data, if possible
- Description of security measures used when processing, if possible

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

GDPR: what to do (in practice?)

Anticipate with impact assessments

- Impact assessments may be required for HIGH-RISK processing.
- New technologies
- Automatic, systematic processing and evaluation of personal information
- Large-scale monitoring of a publicly accessible area (e.g. CCTV)
- Large-scale processing of sensitive data like biometrics

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

GDPR: what to do (in practice?)

The cost of non-compliance

Your local Data Protection Authority monitors compliance; their work is coordinated at EU-level.

The cost of falling foul of the rules can be high:

- Warning;
- Reprimand;
- Suspension of data processing;
- Fine!

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

COBIT

COBIT stands for Control Objectives for Information and Related Technology. It is a framework created by the ISACA (Information Systems Audit and Control Association) for IT governance and management. It was designed to be a supportive tool for managers—and allows bridging the crucial gap between technical issues, business risks, and control requirements. COBIT is a thoroughly recognized guideline that can be applied to any organization in any industry. Overall, COBIT ensures quality, control, and reliability of information systems in an organization, which is also the most important aspect of every modern business.

What is COBIT Framework?

The COBIT business orientation includes linking business goals with its IT infrastructure by providing various maturity models and metrics that measure the achievement while identifying associated business responsibilities of IT processes.

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

COBIT

The main focus of COBIT 4.1 was illustrated with a process-based model subdivided into four specific domains, including:

- Planning & Organization
- Delivering and Support
- Acquiring & Implementation
- Monitoring & Evaluating

All of this is further understood under 34 processes as per the specific line of responsibilities. COBIT has a high position in business frameworks and has been recognized under various international standards. COBIT acts as a guideline integrator—merging all solutions under one umbrella.

The latest **COBIT version 5** came out in April 2012 and consolidated the principles of COBIT 4.1, Risk IT Frameworks, and Val IT 2.0. This version draws reference from IT Assurance Framework (ITAF) from ISACA and the revered BMIS (Business Model for Information Security).

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

COBIT

COBIT 5.0 encourages all organizations to govern and manage information in the most holistic and integrated manner. The guiding principles of COBIT 5.0 are:

- Meeting the needs of stakeholders
- Covering the whole enterprise from end to end
- Application of a single integrated framework
- Ensuring a holistic approach to business decision making
- Separating the governance from the management

Back to Index

ENGINE

Co-funded by the Erasmus+ Programme of the European Union

COBIT

A COBIT 5.0 Certification prepares professionals for the global challenges to the business IT process and also delivers a substantial amount of expertise information on:

- IT management issues and how they can affect organizations
- Principles of IT governance and enterprise IT while establishing the differences between management and governance
- Accessing the ways in which COBIT 5.0 processes can help the establishment of the five basic principles along with other enablers
- Discussing COBIT 5.0 with respect to its process reference model and goal cascade

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

ITIL

The IT Infrastructure Library (ITIL) is a set of books published by the British government's Stationary Office between 1989 and 2014 **to improve IT service management.** The framework contains a set of best practices for IT core operational processes such as change, release and configuration management, incident and problem management, capacity and availability management, and IT financial management.

ITIL's primary contribution is showing how the controls can be implemented for the service management IT processes. These practices are useful as a starting point for tailoring to the specific needs of the organization, and the success of the practices depends upon the degree to which they are kept up to date and implemented on a daily basis. Achievement of these standards is an ongoing process, whereby the implementations need to be planned, supported by management, prioritized, and implemented in a phased approach.

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

ITIL

ITIL was developed by the Central Computer and Telecommunications Agency (CCTA) under the auspices of the British government as a collection of best practices for IT governance. ITIL defines the organizational structure and skill requirements of an IT organization as well as the set of operational procedures and practices that direct IT operations and infrastructure, including information security operations. ITIL continues to evolve. What sets the current version of ITIL apart is the strong focus on end-to-end service delivery and management.

ITIL v4 comprises five main activities or tasks: service strategy, service design, service transition, service operations, and continuous service improvement.

Note: ITIL Certification is only available **to individuals.**

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

COSO Framework

The Committee of Sponsoring Organizations of the Treadway Commission COSO) is a joint initiative of the five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence. It is an international Standard.

COSO identifies five areas of internal control necessary to meet the financial reporting and disclosure objectives. These include:

- Control environment
- Risk assessment
- Control activities
- Information and Communication
- Monitoring

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

COSO Framework

COSO issued the Enterprise Risk Management – Integrated Framework in 2004. This framework defines essential Enterprise Risk Management (ERM) components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management. The guidance introduces an enterprise-wide approach to risk management as well as concepts such as risk appetite, risk tolerance, and portfolio view.

Back to Index

ENGINE

Co-funded by the Erasmus+ Programme of the European Union

NIS (Network and Information Security)

As part of the EU Cybersecurity strategy the European Commission proposed the EU Network and Information Security directive. The NIS Directive (see EU 2016/1148) is the first piece of EU-wide cybersecurity legislation. **The goal is to enhance cybersecurity across the EU.**

The NIS Directive has three parts:

1. National capabilities: EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc.

2. Cross-border collaboration: Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc.

3. National supervision of critical sectors: EU Member states have to supervise the cybersecurity of critical market operators in their country: ex-ante supervision in critical sectors **(energy, transport, water, health, digital infrastructure and finance sector**), ex-post supervision for critical digital service providers (online market places, cloud and online search engines)

SME's are usually not included in NIS directive Compliance, provided that they do not have an "high profile risk" (critical sectors or digital service providers) in that case, NIS directive is valid also for them.

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

NIS (Network and Information Security)

EU Security Network: To improve cross-border cooperation, the Directive will create a network of Computer Security Incident Response Teams (CSIRTs) in each Member State. Member States are also required to designate National Competent Authorities (NCAs) and Single Points of Contact (SPoC) for cybersecurity monitoring, reporting, incident response, and other cross-border coordination.

Member State Strategy: EU Member States are required to implement a national cybersecurity strategy defining security goals as well as relevant policy and regulations needed to enforce the strategy.

Cooperation Group: In addition to the other bodies established by the NIS Directive, there is a further requirement to create a Cooperation Group whose purpose is to facilitate collaboration around cybersecurity between Member States.

Incident Reporting: Those organizations who qualify as DSPs under the Directive's criteria must implement a range of risk management measures both technical and operational. DSP organizations must comply with the Directive's incident reporting protocol, which requires that organizations notify "without undue delay" CSIRTs and other relevant bodies about any significant security incidents encountered.

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

IT Security Certifications

CompTIA Security +

CompTIA Security + is offered to professionals in the IT security sector. Although no prerequisites are demanded, it is recommended that candidates for CompTIA Security + certification have the «Network +» certification or equivalent knowledge; at least 2 years of work experience as an IT systems administrator and as a security officer, daily experience as an IT security technician and a broad knowledge of the main aspects underlying it.

The exam topics, in fact, are decidedly demanding and concern the fundamental principles of network security and risk management. These include Network Security, Compliance and Operational Security, Threats and Vulnerabilities Application, Data and Host Security, Access Control and Identity Management and Cryptography.

https://www.comptia.org/certifications

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

IT Security Certifications

CompTIA CASP

CompTIA CASP certification is an advanced level certification: CompTIA Advanced Security Practitioner is aimed at those who have at least 10 years of experience in IT administration and five years of experience in IT security. CompTIA Advanced Security Practitioner certification attests that the candidate possesses the technical knowledge and skills necessary to conceive and design secure and complex network solutions. The exam topics include challenging subjects such as Enterprise Security, Risk Management and Incident Response, Research and Analysis, Integration of Computing, Communications and Business Disciplines, Technical Integration of Enterprise Components.

https://www.comptia.org/certifications/comptia-advanced-security-practitioner

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

IT Security Certifications

Cisco CCNA Security

Cisco Certified Network Associate (CCNA security) is an ideal certification for anyone looking to pursue a career related to network security. In fact, the certification attests the knowledge and skills at the “associated” level for securing Cisco networks. With the CCNA Security certification, a network professional demonstrates the skills required to develop a security infrastructure, recognize network threats and vulnerabilities and mitigate security threats. The possession of the Cisco CCNA Security certification certifies the ability to install, troubleshoot and monitor network equipment, to maintain the integrity, confidentiality and availability of data and services, and the possession of the skills in the technologies that Cisco uses in its security structure.

https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna.html

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

IT Security Certifications

Cisco Certified Network Professional (CCNP security)

CCNP Security is a highly regarded certification for those working in IT infrastructure field. Cisco CCNP certification identifies a networking professional who can plan, install and maintain converged corporate LANs and WANs, ensuring in-depth knowledge of advanced routing and switching within highly complex networks. In particular, a CCNP certified technician is able to manage routing problems in the implementation of scalable and secure Cisco ISR Routers in both LAN and WAN environments, manage complex LAN solutions using the Cisco Campus Enterprise Architecture including convergence problems, apply structured troubleshooting in solving related problems. It is a suitable certification for those who have at least one year of networking experience and want to take a step forward in their skills.

https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-security-v2.html

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

IT Security Certifications

Certified Ethical Hacker

The Certified Ethical Hacker (CEH) is one of the security certifications that is growing most in popularity. Basically, it certifies ethical hackers, a professional figure who has the same skills as a “Harmful Hacker” but who does not use them to harm the company in which he manages to hack the system; instead, he helps to close security gaps, highlights critical issues and proposes solutions to solve them. It is currently considered one of the most complex technical certifications present due to the amount of requirements both in terms of years of preparation and knowledge required. In order to take the exam, you need to prove at least two years of work experience in IT security.

https://www.eccouncil.org/

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

IT Security Certifications

Certified Information Systems Auditor (CISA).

Certified Information Systems Auditor is recognized and homologated by ISO and ANSI and it is widely used at international level for what concerns Information System and IT Audit competences. It provides technical knowledge, methods and criteria for management, control, security, governance and assurance of IT systems. Among CISA topics, there are: audit processed for IT; IT governance and management; IT system development and operations; Maintenance and Support and protection for IT systems. At least 2 years of experience in IT systems is required.

https://www.isaca.org/credentialing/cisa

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

IT Security Certifications

Certified Security Manager (CISM)

The Certified Security Manager (CISM) is an ideal certification for experienced IT managers, security managers and CSOs. The professional in possession of this certification is essentially a manager who promotes international safety practices. It is in fact a professional figure who directs, designs, supervises and evaluates information on the safety of a company. The objectives of the CISM exam include subjects such as access control, identity management, security management, policies and procedures, intrusion prevention, network security, physical security, security tools and security trends.

https://www.isaca.org/credentialing/cism

Back to Index

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

IT Security Certifications

Certified Information Systems Security Professional (CISSP)

The Certified Information Systems Security Professional (CISSP) is one of the most prestigious certifications in the field of information security, so it represents a standard recognized worldwide. Professionals in possession of this certification certify that they have acquired knowledge and skills for the development of IT security policies, rules and procedures to put their implementation into practice throughout the company. The exam includes tests to be passed in topics such as: Security & Risk Management; Asset Security; Security Engineering; Communications & Network Security; Identity and Access Management; Security Assessment & Testing; Security Operations; Software Development Security. A certification, needless to say, that is aimed exclusively at Information Security professionals.

https://www.isc2.org/Certifications/CISSP

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

IT Security Certifications

CCSP (Certified Cloud System Professional)

Without a doubt, cloud technology is changing the way cybersecurity professionals protect corporate infrastructures. That's why security professionals are increasingly looking to a certification like the Certified Cloud Systems Professional (CCSP). This certification demonstrates in-depth knowledge of how cloud applications and platforms operate and the ability to ensure security of the data infrastructure. This last point is particularly delicate and important because, by entrusting their data to an external platform, end customers demand the maximum possible protection. With the arrival of the GDPR in April 2018, this certification has even more importance on compliance, audit processes and privacy issues.

https://www.isc2.org/Certifications/CCSP

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

IT Security Certifications

Certified Secure Software Lifecycle Professional (CSSLP)

The field of software development is growing exponentially. Hence, the high demand for software is creating even greater demand for those who have the ability to keep software and applications safe. This is enough to explain the growing success of the Certified Secure Software Lifecycle Professional (CSSLP). Note that the exam qualification requires at least four years of full-time work as a Software Development Lifecycle (SDLC) professional.

https://www.isc2.org/Certifications/CSSLP

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

Sources

- ISO2700 standards:
  - https://www.iso.org/ics/35.030/x/
  - https://advisera.com/27001academy/iso-27001-controls/
  - https://www.iso27001security.com/html/27001.html
  - https://www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards
  - https://www.dnv.com/services/iso-iec-27701-international-standard-for-privacy-information-management-159186

- GDPR
  - https://gdpr.eu/what-is-gdpr/
  - https://www.itgovernance.co.uk/blog/gdpr-for-small-business-the-ultimate-guide
  - https://protezionedatipersonali.it/regolamento-generale-protezione-dati

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

Sources

- COBIT
  - https://www.isaca.org/resources/cobit
  - https://www.simplilearn.com/what-is-cobit-significance-and-framework-rar309-article
- ITIL
  - http://www.itil-officialsite.com/
- COSO Framework
  - https://www.coso.org/Pages/default.aspx

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

Sources

- NIS
  - https://www.enisa.europa.eu/topics/nis-directive
  - https://eur-lex.europa.eu/eli/dir/2016/1148/oj
  - EU Cybersecurity strategy
  - EU 2016/1148

- IT Security certifications
  - https://www.comptia.org/certifications
  - https://www.comptia.org/certifications/comptia-advanced-security-practitioner
  - https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna.html
  - https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-security-v2.html
  - https://www.eccouncil.org/

Back to Index

Co-funded by the
Erasmus+ Programme
of the European Union

Sources

- IT Security certifications

  - https://www.isaca.org/credentialing/cisa
  - **https://www.isaca.org/credentialing/cism**
  - https://www.isc2.org/Certifications/CISSP
  - https://www.isc2.org/Certifications/CCSP
  - https://www.isc2.org/Certifications/CSS

Back to Index