DG DIGIT
Unit S1 – IT Security Policy

Global approach to Security Processes

S²LC – IT Security in System Life-Cycle

Date: 01/06/2019
Doc. Version: v2.4

Document Control Information

Settings	Value
Document Title:	Description of the S²LC
Project Title:	S²LC – IT Security in System Life-Cycle
Document Author:	DIGIT.S1.IAO
Doc. Version:	v2.4
Sensitivity:	Final
Date:	01/06/2019

TABLE OF CONTENTS

1 INTRODUCTION

The goal of IT security in the Commission is to ensure that the Commission's […] Systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.[1]

This high-level goal of IT Security is extracted from Commission's legal base on IT Security. It is further refined in its Implementing Rules and detailed in accompanying standards.
The present document do not substitute to these requirements. It should be considered as a **guideline** to position pragmatically all the security requirements mandated in the legal bases in the global life-cycle of any IT System, from its inception to its decommissioning.

Achieving this goal in practice relies on five main principles:

1. Consider security as a global process, not as a product, and consider security measures as **processes** to implement in an organized way; for example, encryption is a process that can be implemented in a system to protect information in transit;
2. **Instilling** security processes throughout the whole **life-cycle** of the system/information, at the correct place and moment, from initiation to end of life;
3. **Defining** appropriately these security processes by following a **risk-based approach** (itself a process);
4. **Managing** these security processes (Management System) and
5. **Improving continuously** these security processes to ensure they stay appropriate during the whole life-cycle (a.k.a. Deming virtuous cycle, or PDCA for PLAN-DO-CHECK-ACT).

This document provides a global view on the security processes required to implement these principles to develop and operate appropriately protected Systems, from their inception to their decommissioning. It will be complemented by various topic-specific documents detailing how to implement these security processes.

It is commonly admitted that Security Processes can be **categorised** as:

1. "**Corporate Processes**" which are implemented at corporate level and are valid for all systems, e.g. defining a Global Security Policy;
2. "**Life-Cycle Processes**" which are implemented during development and operation of the system to increase assurance to have a secure system, e.g. performing a Risk Assessment on the system;
3. "**Functional Processes**" which are implemented and running as part of the system or organization to mitigate assessed risks, e.g. encrypting data;
4. "**Management and Supporting Processes**" which are used to manage or support "Functional Processes", e.g. management of encrypting keys; these can usually be considered as sub-processes.

This document focuses on Life-Cycle Processes as part of IT Security in System Development and Operation. Other processes are performed either at organization level or are part of the system or supporting it, and will not be described in this document.

[1] Commission Decision 46(2017) concerning the Security of Communication and Information systems in the European Commission, Art. 3 1)

2 IT SECURITY IN SYSTEM LIFE-CYCLE (S²LC)

2.1 System Life-Cycle (SLC)

The Life-Cycle of an IT System (System Life-Cycle – SLC) is the set of all phases of its existences, from its initiation to its end of life. It may be roughly divided into two main sub-cycles:

(1) ***the System Development Life-Cycle (SDLC)*** usually includes initiation, requirements analysis, design, development, integration, tests and release to operation; these processes are performed in Project Management mode; their details and the way they are articulated is part of *Software Engineering* and *Project Management disciplines*;

(2) ***the System Operation Life-Cycle (SOLC)*** usually includes system deployment, operation, management, maintenance, and finally retirement and disposal; these processes are performed in Service Management mode; their details and the way they are articulated is part of *Service Management* frameworks.

There are plenty of Project Management methodologies, of Software Engineering *methodologies*, and of Service Management *frameworks*.

In practice, IT Systems are developed and operated by implementing different processes which are defined, organized and ordered following project management, software engineering and service management methodologies.

For example, Software Engineering methodologies may propose a waterfall model, a V model, a W model, an iterative model, a spiral model, or an agile model. And each model defines different processes, may split them in different sub-processes, and may propose to perform them in different order and in different iterations. But all methodologies and framework will contain the basic processes quoted above.

Nowadays, a better and smoother integration of these two Life-cycles (SDLC + SOLC) is proposed in **DevOps** concept.

2.2 IT Security in SLC (S²LC)

To develop and operate IT Systems providing appropriate protection of the information they process, System Life-Cycle Security Processes must be inserted smoothly along the processes of its development and operation life-cycles (SDLC + SOLC).

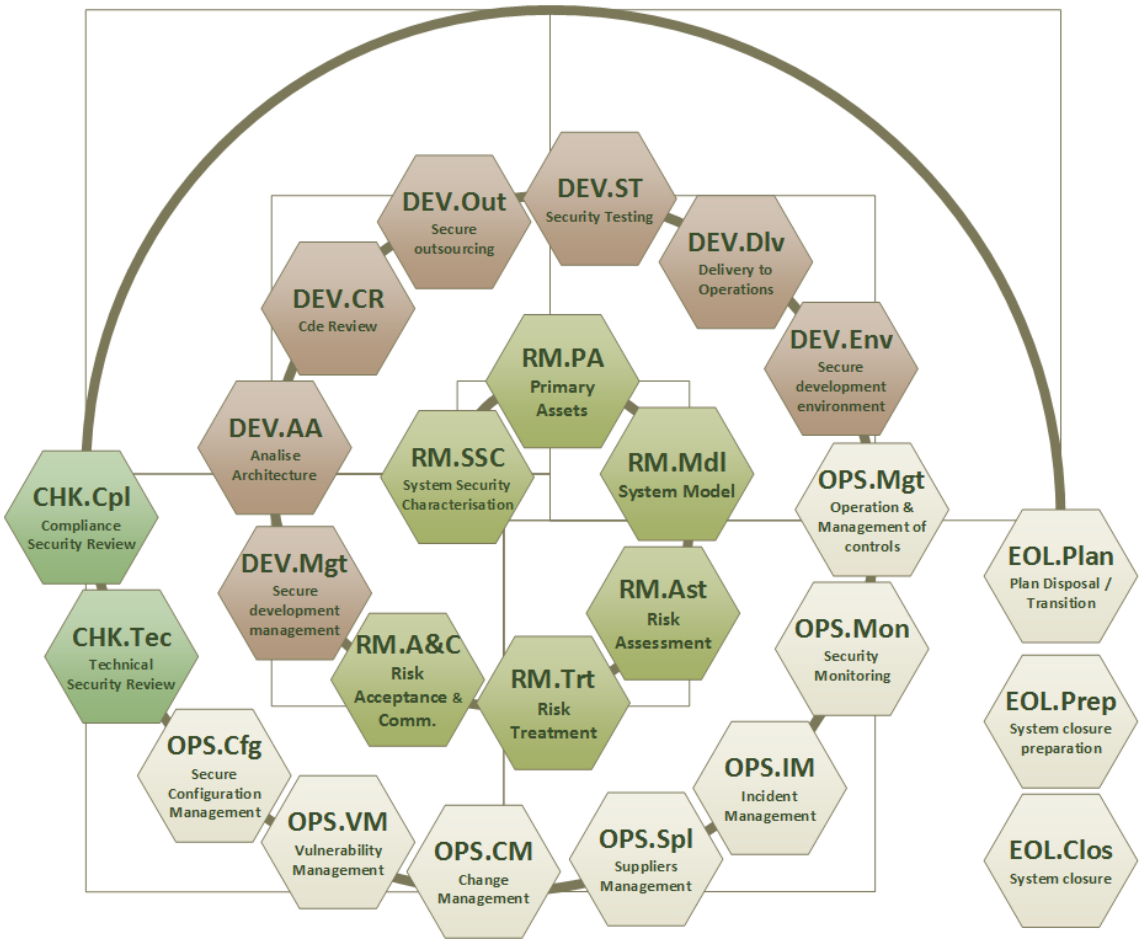
Depending upon the methodologies and frameworks used, these Security Processes will be performed in different sequence, following the sequence provided for development and operational processes, but their definition and organization remains broadly the same. This is why, in the rest of this document, the sequence in which these Security Processes will be defined is only the linear organisation of the document and not bound to the sequence of any methodology or framework. They can be, later on, refined and smoothly instilled in the sequence of the specific System Life-Cycle chosen by the Development Team and the Operation Team. To demonstrate this possibility, the S²LC will be injected into the E2E (End-to-End) meta-framework.

Such insertion of security in DevOps is also aligned with the concept of **DevSecOps**.

System Life-Cycle Processes may be divided into five groups:

(1) [RM] - IT Security Risk Management Processes (including [IR46/2017] Art.5): analyzing security needs and deriving the security requirements to define an IT System providing appropriate protection for the data it processes. This corresponds to a **PLAN** iteration.
(2) [DEV] - Secure IT system development and acquisition Processes (including [IR46/2017] Art.8): required to add security in development and to develop security controls identified in previous group (Risk Management). This corresponds to a **DO** iteration (implement security) or to an **ACT** iteration (correction or maintenance of security).
(3) [OPS] - Secure IT system operations Processes (including [IR46/2017] Art.6&7): day-to-day Security Processes ensuring and maintaining security of the System, and processes managing security controls implemented in the previous phase.
(4) [CHK] - IT Security compliance Processes (including [IR46/2017] Art.10): measuring security in systems. This corresponds to a **CHECK** iteration.
(5) [EOL] - Secure IT system decommissioning Processes: decommissioning steps required before End Of Life of the system. This could be considered as a "last **DO**" iteration.

3 LIFE-CYCLE PROCESSES



A spiral has been chosen to express that the S²LC is not at all limited to waterfall or V or W model, but can be executed in any sequence best fitting the actual life-cycle of a system, can be started at any point, and will iterate in a PDCA continuous improvement cycle.

3.1 [RM] – CIS Security Planning – Assess IT Security Risks and Define Risk Treatment Plan

Applicable references	
Standards	Information Security Risk Management (CD3602)
Guidelines	ITSRM² (IT Security Risk Management Methodology) - Description of the methodology
Services	DIGIT.S1.IAO: ITSRM² Review service DIGIT.S1.IAO: ITSRM² Coaching service HR.DTS: ITSRM² Practitioner Training (via EU Learn)
External	ISO 27005 (Information security risk management) ISO 27001 (Information Security Management System – Requirements) NIST SP800-64 (Consideration in the System Development Life Cycle)

The main initial process in system development consists in capturing what users want from the system (their needs) and in specifying what will have to be implemented to fulfil these

needs (the requirements). This is usually referred to as functional analysis process because the majority of the needs and requirements are functional (what the system should do and which functions should be implemented to do it). But there are also non-functional needs and related requirements which must be captured and specified. This is the case for quality, ergonomics, user-friendliness or performance. And this is also the case for IT Security which should be integrated as other (non-)functional needs and requirements within development project management and software engineering methodologies.

There are techniques to capture functional needs and specify appropriate required functions to be developed to fulfil these needs. The same way, there are techniques to capture security needs and choose and define appropriate security controls to fulfil these security needs: this is the field of IT Security Risk Management.

The **main** processes of IT Security Risk Management are described hereafter, and can interact as follows:

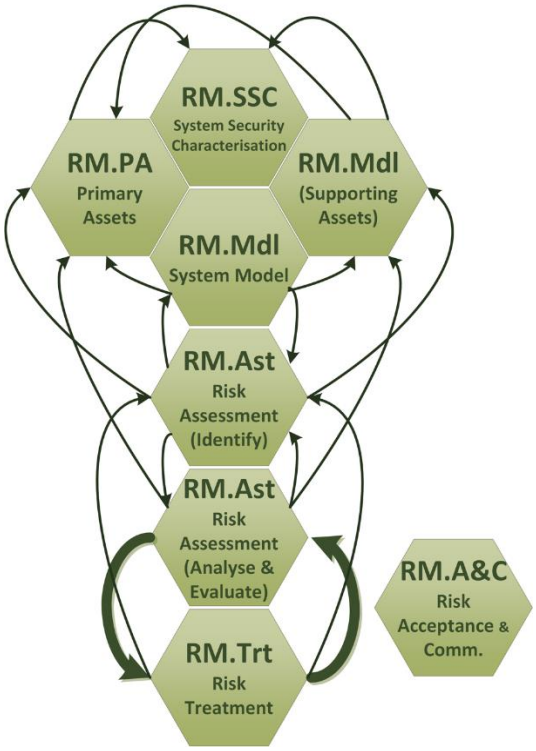


Figure 1 - Security Processes of IT Security Risk Management

This picture shows that Risk Management processes are highly iterative, can be updated whenever additional information is available, and should be updated whenever there is a change in the system (e.g. new data processed with different sensitivity, changes in the system, change in threat landscape).

In addition, RM processes are subject to the PDCA cycle and should be reiterated regularly as part of continual improvement cycle.

3.1.1 RM.SSC – System Security Characterization

The *aim* of this process is to provide a high-level description of the CIS and its context and a maximum of information concerning its development which will be helpful for the analysis and implementation of its IT security.

The *Outcomes* of this process are:

- A description of the organization for which the CIS is developed;
- A high-level description of the CIS;
- A list of the *main constraints* affecting the organization and the system, in order to determine security requirements that are mandatory. These constraints will contain at a minimum the requirements from [CD443/2015], [CD444/2015], [R45/2001] and [CD46/2017];
- A list of the *mandatory security measures* applicable to the system, taking into consideration the *main constraints* to the system identified before;
- A nomination for *security roles* as defined in [CD46/2017].

These descriptions should be synthesized and focused on elements which could have an impact on IT security.

3.1.2 RM.PA – Primary Assets

In IT security, primary assets are assets which have a business value, and not only a financial value, because they bring value to the business. We will consider two types of primary assets:

1) *Data Sets*[2] or *Data* (for short) managed by the IT System and
2) *Functions*[3] provided by it

which are vital for accomplishing the mission of the organization.

The *aim* of this process is to identify primary assets in the system, to describe them, to identify their owners, to assess their value to business, and to gather different characteristics about them that will help in managing the risks they will face.

In IT security, Asset Valuation is often done by evaluating the business impact the organization would suffer in case of loss of Confidentiality, Integrity and Availability (C/I/A) of the asset. This process is also known as Business Impact Assessment (BIA).

The asset value in terms of Confidentiality, Integrity and Availability (C/I/A) conditions the level of protection the asset requires against loss of its C/I/A; so this is often described as the "security needs" of the asset.

3.1.3 RM.Mdl – System Model

The *aim* of System Modelling is to build a representation of the system which will ease identification and then treatment of the risks.

A system model is built by identifying and describing its components, called supporting *assets*, and by defining how they are interrelated to process primary assets.

[2] [CD46/2017]: A Data Set is a set of information which serves a specific business process or activity of the Commission.

[3] [CD46/2017]: The processing of information comprises all functions of a CIS with regard to Data Sets, including creation, modification, display, storage, transmission, deletion and archiving of information. Processing of information can be provided by a CIS as a set of functionalities to users and as IT services to other CIS.

The following main types of supporting assets should be considered:

1) Hardware: physical element of the CIS contributing to the processing, transmission or storage of primary assets (e.g. workstation, server, communication media, storage media);
2) Software: CIS software contributing to the processing, transmission or storage of primary assets (e.g. end-user application, middleware, operating system, firmware);
3) Personnel: people using the CIS or involved in the processing, transmission or storage of primary assets (e.g. end-user, developers, operation staff, decision makers);
4) Services: data processing capabilities offered by a subset of hardware, software, personnel or by (sub)services (e.g. Network Services, Hosting services, Cloud Services);
5) Location: physical place where hardware, software and people are located.

3.1.4 RM.Ast – Risk Assessment

The *activities* for this process are the identification, analysis and evaluation of risks.

1) The first activity in this process is to identify risks the CIS is facing, usually by defining risk scenarios. A risk scenario regroups one or more *Primary Assets*, one or more *Security Dimensions* (Confidentiality, Integrity, Availability), *a threat* that can harm the Security Dimension and the *Supporting Assets* where the Threat materializes.

2) Now that security risks have been identified, their level can be assessed through a Risk Analysis. During Risk Analysis, the level of risk is computed as a combination of the likelihood of the risk scenario and its consequences in case it materializes. Both, the Inherent and Residual risk levels will be computed during Risk Analysis. The Inherent risk is the risk before treatment, when no security measures are taken into account. The Residual risk is a reduced value of the Inherent risk level, due to selection of Security Measures to modify / reduce risks.

3) During Risk Evaluation, risks are presented in comparison with risk criteria (prioritized by risk level and compared to risk level that could be accepted) to ease decision making about risk treatment.

The *Outcomes* of the RM.AST process, are:

- A risk register presented as a list of risk scenarios identified and populated with the inherent and residual risk levels.
- A risk catalogue with risks prioritized by residual risk level (to ease acceptance choice).

3.1.5 RM.Trt – Risk Treatment (definition of Security Requirements)

The *aim* of this process is to choose the most appropriate way (treatment option) to address the risks that could prevent the CIS from achieving its business objectives. Addressing a risk means in most cases reducing it, but it can also mean accepting it or increasing it in exchange for a larger overall benefit.

The *activities* of this process are:

1. Formulate risk treatment options (Modification, Retention, Avoidance, Sharing);
2. When Modification option is chosen: identify the possible Security Measures (Security Controls) that may be a viable response to modify (reduce) the risk;

3. Consolidate the Risk Treatment Plan (including the set of the proposed Security Measures chosen to reduce risk up to an acceptable level, in case the treatment option chosen is mitigating the risk), together with corresponding Residual Risks;

The *outcome* of this process is the proposed Risk Treatment Plan, reflecting the corresponding Residual Risks.

3.1.6 RM.A&C – Risk Acceptance and Communication

The *aims* of this process are:

- To obtain the approval from the System and Data Owner for the proposed Risk Treatment Plan according to (Residual) Risks provided; and
- To communicate to different target audiences the approved Risk Treatment Plan and/or Residual Risks, possibly filtered/ arranged per audience type.
- To identify the possible strategy – Acquisition or Development – to be used further in the DEV Process, based on a specific analysis performed

The *Outcomes* of this process, grouped on the interests of different target audiences, are:

- For IT Teams: security measures approved are provided to the IT teams for implementation;
- For Head of the Commission department: a regular report to the head of the Commission department on the IT security risk profile of their CIS;
- For DIGIT:
  - a summary of IT security risks and measures is reported on a regular basis to DIGIT;
  - a report to DIGIT on the related risks, risk management activities and security measures taken.
- For the Information Systems Security Officer role and the development team, the decision on the Strategy to be used in the Development Process: Acquisition or Development.

3.2 [DEV] – Secure IT system development & acquisition – Design and Implement a Secure CIS

Applicable references	
Standards	Web application security standard (New) Secure systems development (3602, new to come) Principles and rules for outsourcing of CIS (HR.DS)
Guidelines	Web Application Secure Development Guidelines (3602)
Services	DIGIT.S1.SA: Dynamic analysis of deployed web applications DIGIT.S1.SA: Static analysis of source code DIGIT.S1.SA: Black Box Infrastructure Vulnerability Assessment DIGIT.S1.SA: White Box Infrastructure Vulnerability Assessment DIGIT.S1.SA: Black Box Infrastructure Penetration Testing DIGIT.S1.SA: White Box Infrastructure Penetration Testing
External	BSIMM (Built Security In Maturity Model) NIST SP800-53 (Security and Privacy Controls for Federal Information Systems and Organisations) NIST SP800-64 (Consideration in the System Development Life Cycle) ISO 27001 (Information Security Management System – Requirements) NIST SP800-115 (Technical Guide to Information Security Testing and Assessment)

In this process, the requirements captured in the [RM] process are implemented and injected into the system, from its detailed design to its release into production in a state where it can be operated. Throughout this process, attention must be given to developing a secure system: when designing the system, developing the system, testing the system and handing it over to the teams that will operate it.

Security processes that mirror those different sub-phases of the System Development & Acquisition phase exist: they must be adequately executed to ensure that the CIS is secure, and the controls documented in the Risk Treatment Plan are implemented. These security processes interact as follows:

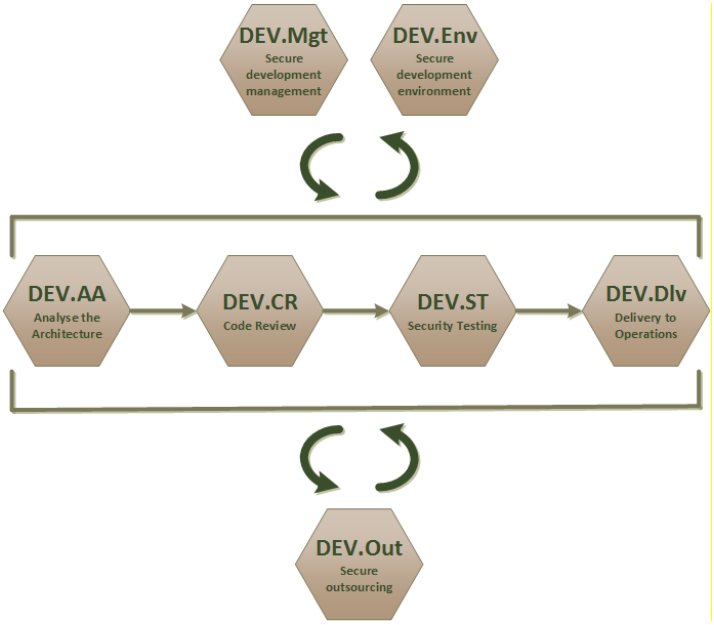


Figure 2 - Secure IT system development & acquisition Processes

3.2.1 DEV.Mgt – Secure Development Management

The *aim* of this process is to decide on the Development Strategy and ensure the proper management of the security aspects during the System Development & Acquisition phase, and the informed and risk-based decision-making on matters that relate to the security of the System produced.

The *activities* of this process are grouped in (1) initial activities, performed before the start of the development and (2) ongoing activities aimed at ensuring the effectiveness of the other security processes in this phase.

1. The *Initial activities* and their related Outcomes, consist of:

- Document and design all Security measures to be implemented in CIS life-cycle and required to meet the IT security needs of a CIS;
- select security competences to require of the CIS developers and other project participants and the training activities to carry out
- allocate information security and development roles and responsibilities to project participants ; this includes the identification of incompatible duties and the definition of measures to ensure their separation;
- define a calendar of security test activities (milestones) in relation to the development calendar, as well as the interaction between the two;
- select internal and external technical standards to follow, which may be driven by compliance to (regulatory) constraints identified in RM.SSC;
- select security tools to use;
- define Secure Code Practices that should account for all types of software development languages used;
- define security metrics to use in evaluating the effectiveness of the security processes implementation and in go / no go decisions, as well as the way to measure and present evidences for the performance of the processes along those metrics.

2. The *Ongoing activities* and their respective *Outcomes*, are:

- The Quality Management activities (planning, assurance and control), for ensuring minimal defects within the information system (e.g. ensure control on changes brought to the security controls in the development phase, ensure bad coding practices are not used or ensure quick remediation of the weaknesses known). They reduce gaps that can be exploited or misused, causing vulnerabilities in the system.
- The monitoring of the implementation of the measures defined during initial activities;
- The monitoring of the execution of the other security processes of the Development & Acquisition phase;
- Records of the course correction decisions taken during the governance meetings based on that input.

3.2.2 DEV.Out – Secure Outsourcing

Parts of the System may be realised through procurement from a supplier, as a service from a provider (or a chain of suppliers and providers). The Commission is accountable for the creation of a secure System, while the external party is responsible for it.

The *aim* of this process is to carry out the controls necessary for ensuring that components delivered by external parties implement the Security identified in the [RM] activities, in a fashion that aligns with the DEV.AA, DEV.CR and DEV.ST processes - to the extent that these are the responsibility of the outsourcing party.

The following *activities* are specifically required to support this objective:
- Include security provisions in the agreements with the external parties;
- Monitor outsourced activities and enforce secure development practices by the suppliers, including the effective execution of all activities outlined in DEV.Sec – Secure Development, by the external party;

3.2.3 DEV.AA – Analyse the Architecture

The *aim* of this process is to eliminate security mistakes from the foundations of the CIS, because they could be much more costly to eliminate later. The aim is achieved by involving security people early in development, while architecting the system and carrying out with them security related activities on the architecture.

The *activities* are:

- *Perform security feature review*: The security features of the System are based on the Security Measures identified during the [RM – CIS Security Planning] phase. Security reviewers study the design (at various stages of finalization) of the System, looking for problems that would cause these features to fail at their purpose or otherwise prove insufficient.
- *Perform design review*: Experienced security reviewers review the entire design of the CIS in detail (not just the security features) and produce a report of flaws found and remediations recommended. As opposed to a Risk Management exercise, which is systematic and starts from the assets that need to be protected, the design review relies more on the reviewers' experience with the technology and with architectural anti-patterns.

- *Define secure configuration requirements*: Where pre-existing system components are implemented or customized, define secure configuration requirements for each of these components. This includes all middleware and infrastructure components deployed to support the System.
- *Define and use an Architecture Analysis process*: In this activity a methodology for performing design reviews is documented, standardizing how to think about attacks, security properties, and the associated risk. The methodology is defined rigorously enough such that non-security people can be taught to carry it out.
- *Standardize architectural descriptions (including data flow)*: This activity establishes an agreed-upon format to describe the CIS in terms of structure and behaviour, including a means for representing data flow. The format may be specified in an external standard or in an internal document.
- *Have software architects lead design review efforts*: In this activity the organization appoints software architects to lead the Architecture Analysis effort. The rationale is that they already master non-security Architecture Analysis methodologies and they have the experience required to break architectures and provide solutions. Security experts can help Architecture Analysis in an advisory capacity.

3.2.4 DEV.CR – Review the Code

The *aim* is to eliminate security mistakes at the source code stage in order to avoid having to eliminate them in later stages, which can be much more costly. The aim is achieved by carrying out analysis of the source code of a CIS (without execution) with the purpose of discovering security flaws it may contain. It includes the use of code review tools and the customisation of their behaviour to the System to which they are applied and to the role of the person using the tool.

The *activities* are:

- *Perform ad-hoc code review by security experts*: have the relevant security experts proactively and opportunistically reviews the source code (manually or assisted by tools).
- *Automated code reviews*: Employ static analysis tools to complement manual security code reviews in order to achieve larger scale, better coverage and a minimum level of security expertise necessary when the human reviewers are inexperienced.
- *Use centralised reporting to close the knowledge loop and drive training*: The results of code reviews are not only distributed to the team that will implement the fixes, but are also tracked in a centralized repository together with the results from the code reviews of other code reviews. This ensures that the organization can have an overview of the results, can identify systemic weaknesses and can measure trends.
- *Assign tool mentors*: Certain persons will develop more expertise than others in the use of the specific static analysis tools used during the development of the CIS. The other team members would also benefit from access to such expertise, therefore the tool expert should be identified, designated as tool mentor and brought to the attention of the other team members.
- *Tailor rules of automated tools*: Static analysis tools start out of the box with generic detection rules. By tailoring the configuration and rules of the software it can be made to run more efficiently, waste less developer attention and achieve better insight into the source code of the CIS.
- *Automate malicious code detection*: This activity is a specialization of the activity above for tailoring the rules of automated code review tools.

3.2.5 DEV.ST – Test the Security

The *aim* is to take advantage of certain unique characteristics of vulnerability discovery though security testing. Vulnerability discovery has a high degree of credibility, since it shows the vulnerability being exploited, and it can catch vulnerabilities not present in the source code, but introduced at build time.

The aim is achieved through a variety of pre-release testing for security vulnerabilities (with execution and various inputs), including the integration with standard Quality Assurance (QA) testing. Tools and techniques include black-box testing (no knowledge about the source code is used), risk-driven white-box testing (a search for vulnerabilities guided both by knowledge about the system's internals and by the knowledge of the most severe risks), application of the attack model etc.

The *activities* are:

- *Integrate security requirements and security features in QA*: The regular QA process must be leveraged to include security testing, by feeding it the security requirements and the intended behaviour of the security features.
- *Ensure QA supports edge/boundary value condition testing*: The exploitation of many vulnerabilities happens when the system is pushed by the adversary beyond the limits it has been designed to handle. Those are the edge/boundary conditions and they do not require security knowledge to understand. By having the regular QA process test the CIS in those conditions, too, they can offload that task from the security specialist testers, who can concentrate on testing which requires security expertise.
- *Integrate black-box security tools into the QA process*: While black-box security testing tools encapsulate security knowledge, they are used to their maximum potential only when they are part of the development lifecycle like functional testing is. This activity ensures that they are managed as part of the QA process in terms of inputs, moments when the tests are triggered, how the results of the tests are transformed into work tasks for developers etc.
- *Share security results with QA*: Share the results of security reviews performed outside the QA process with the QA team, enabling them to evolve their testing patterns and learn the security mindset.
- *Include security tests in QA automation*: Integrate security testing even closer into the QA process than in the activity above by including security tests into the automated regression test suite. This will ensure that they discover vulnerabilities soon after the code is committed, shortening their lifetime.

3.2.6 DEV.Dlv – Delivery to Operations

During this process, the system will be installed and evaluated in the organization's operational environment.

The *aim* of this process is to ensure that the System enters operation fully implementing the controls from the Risk Treatment Plan (RM.Trt).

The *activities* of this process are:

- Develop the documentation and training materials for secure deployment, operation and disposal; user manuals concentrating on the role users can have in security can also be useful;
- Configure the System in a secure initial state;
- Test the security controls implemented;
- Integrate the CIS into the operational environment;
- Approve System Deployment.

3.2.7 DEV.Env – Secure development environment

A secure development environment lends itself to developing secure software and systems. It includes workstations, servers, network devices, and code repositories.

The *aim* of this process is to ensure that the development process itself is not subverted by accident or maliciously.

Operational security *activities* during the [DEV] process are:

- Setting up and maintaining a secure development environment, adequately isolated, controlled and protected;
- Carefully selecting test data; they should not contain any sort of confidential information, including data which assembled with other sources could constitute private data; they should be fictitious or anonymized;
- Controlling access to source code;
- Controlling changes to the master copy of the source code;
- Managing information system accounts for roles specific to ensuring information security as part of CIS, and roles specific to the development or acquisition of the CIS: approval, creation, modification, deactivation and removal of accounts. This activity is supporting the performance of the previous activities;
- Approving the development environment(s).

3.3 [OPS] – Secure IT system operations – Maintain CIS Security

Applicable references	
Standards	IT Asset management (New) Information systems security Incident management (3602) Logging and monitoring (3602) IT Vulnerability and Remediation Management (New) Operational management (3602)
Guidelines	ITSRM² Business Impact Level Scale to IT Asset Priority Label Mapping (New) Security incident management and incident notification (3602) Vulnerability Management process
Services	DIGIT.S1.SA: IT Vulnerability Management DIGIT.S2.SMON: Security Monitoring DIGIT.S2.CSIRC: Computer Security Incident Response
External	BSIMM (Built Security In Maturity Model) NIST SP800-53 (Security and Privacy Controls for Federal Information Systems and Organisations) NIST SP800-64 (Consideration in the System Development Life Cycle)

	ISO 27001 (Information Security Management System – Requirements) ISO 27035 (Information Security Incident Management) ITIL (Information Technology Infrastructure Library)

In the OPS process, the functioning CIS is creating value for the organization until it will be disposed of. Unlike during the [DEV] process, the CIS is now active in a dynamic environment and operates with the security measures defined in the [RM] process. The CIS now changes through configuration, rather than development.

The [OPS] security processes contribute to the secure operation of the CIS, but also the monitoring thereof, and the management of potential security incidents, as illustrates the following diagram:

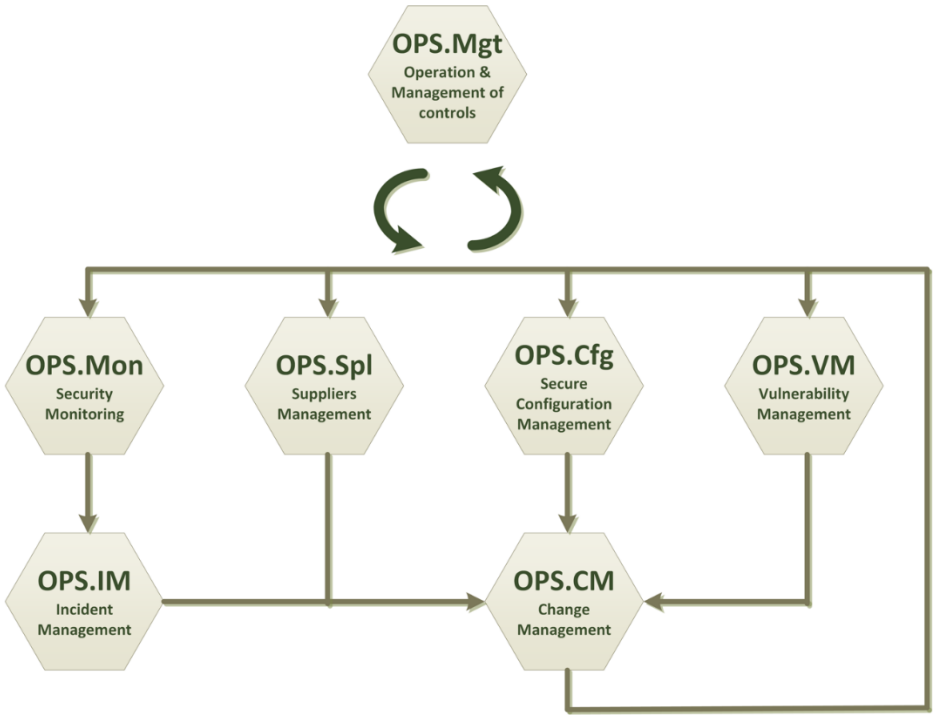


Figure 3 - Security Processes of the OPERATE phase

3.3.1 OPS.Mgt – Operation and management of Security Measures

The *aim* of this process is to operate and manage Security Measures identified during the RM process (in Risk Treatment Plan and documented in DEV.Mgt in Security Controls Plan) and implemented in the following [DEV] processes. By the means of the security controls implemented, CIS has a better chance of withstanding threats and recovering with minimal loss from materialized risks.

The *activities* that support the operation and management of the Security Measures:

1. Coordination and Operation

- Operate the Security Measures (or Security Controls) implemented in DEV.Sec Secure Development Process or DEV.Out Secure Outsourcing, in line with the specific criteria established in the Security Controls Plan

- Evaluate if the roles for the operation of Security Measures (security controls) perform the assigned activities as intended
- Coordinate actions for efficient operation of controls
- Log security controls operation performance for further analysis/ evaluation

2. Performance Evaluation

- Monitor, measure and assess the efficiency and effectiveness of the implemented security controls. The processes CHK.Tec Technical Security Review and CHK.Cpl Compliance Security Review will be employed in support to this activity.

3. Performance Improvement

- Identify security controls that do not perform in accordance to the established criteria;
- Identify the causes for the poor performance of the control/ security measure, and the implementation phase they relate to (design, development or operation phase);
- Plan changes to security controls in order to address the deficiencies identified in their design, development or operation, in accordance to OPS.CM Change Management;
- Implement and control the planned changes brought to the Security measures.

3.3.2 OPS.Mon – Security monitoring

The *aim* of this process is to ensure that when risks materialize, they are promptly detected, allowing process OPS.IM 'Incident Management' to handle them.

This includes:
- log collection and correlation,
- behavior anomaly detection,
- generation of security event candidates,
- possibly machine learning solutions that make use of security events collected in order to identify and propose behavior patterns for analysis.

The scale of data security monitoring has to consider in a modern system means, what used to be carried out manually in the past has to be automated as much as possible.

The *activities* left to human operators and analysts are:
- Configuration of the parameters of security monitoring;
- Validation of security event candidates;
- Initial triage of security events by impact level.

3.3.3 OPS.IM – Information Security Incident Management

The *aim* of information security incident management is the restoration of the secure state of the system with a minimal amount of loss.

Incident management can be broken down into:
- Activation of the incident response plan by notifying the persons with assigned roles in incident response, making the resources available for incident handling;
- Communication, both internal and external, allowing employees, business partners, oversight organisms, law enforcement and the general public to receive the appropriate information, which is sometimes prescribed by regulation;

- Investigation of the incident in order to learn its true extent and provide sufficient information for the responders to carry out the next activities;
- Containment of the threat, to keep the threat both from re-entering the system and from spreading further in the system to cause additional security incidents;
- Eradication of the treat, to ensure that no element of the threat is present anymore in the system, able to make the risk materialize again;
- Recovery, consisting of restoration of any disrupted services, replacement or restoration of the unavailable assets (replacement computers, data restored from backup), resuming the processes affected by the incident;
- Learning from incidents, which goes beyond restoring the secure state by any means (the previous activities) and addresses root cause analysis and systemic remediation.

3.3.4 OPS.Spl – Supplier management

The *aim* of supplier management is to ensure protection of CIS assets accessible by suppliers and maintain an agreed level of service delivery in line with supplier agreements for CIS.

The *activities* specific to Supplier Management are:
- Define, monitor and control supplier access to CIS assets and the types of information accessed by them;
- Monitor and review services delivered, and actions performed by suppliers, including the assurance that the supplier maintains sufficient service capability to deliver the services;
- Implement rules for handling incidents and contingencies associated with supplier access;
- Establish resilience, recovery and contingency arrangements with suppliers, to ensure the availability of the information or information processing provided by either party;
- Manage transition of information and information processing facilities with suppliers;
- Manage changes to supplier services during the OPS.CM Change Management Process. This includes changes to the service provisions and the improvement and maintenance of the controls and procedures that apply to the agreements with suppliers.

3.3.5 OPS.CM – Change management

The *aim* of Change management Process is to ensure that changes brought to CIS during its whole life-cycle, are done in a controlled manner and with an audit trail;

The *activities* specific to Change Management are:
- Design and Implement a change management framework that will ensure: identifying significant changes to CIS, planning and testing for changes, assessing security impacts of changes, approving changes, assessing the alignment with the security requirements after change, treatment procedures for emergency and critical changes, or fallback/ abort/ recovery procedures from unsuccessful change;
- Restrict unauthorized changes to CIS' operational environment by segregating environments (development, test and operational);
- When changes are brought to high importance infrastructure elements like operating systems or databases, review and test CIS critical components that rely on them, to ensure there is no adverse impact on CIS operations or security;
- Limit and control modifications to software packages;
- Manage changes to supplier services and service provisions.
- Manage changes to Business Continuity Plans arising from test results for these plans and other factors that affect the Business Continuity Process.

3.3.6 OPS.VM –Vulnerability Management

The *aim* of the Vulnerability Management (VM) process is to coordinate the activities that will remediate major vulnerabilities identified in Commission IT Systems.

Patch and Vulnerability Management employs a set of activities that will ensure in-time identification, evaluation and remediation of CIS vulnerabilities. Here, an important role is played by the asset manager which will ensure the resources (personnel, actions and tools) necessary to detect CIS vulnerabilities and will ensure the monitoring and resolution of CIS vulnerabilities.

The following are the *activities* employed by the VM process:

- Vulnerability Monitoring and Applicability Check, which focuses on monitoring for new vulnerabilities and ensuring that those affecting EC are adequately analyzed and handled.
- Recording and Risk Assessment, which is focused on recording vulnerability instances and assessing their risk.
- Strategy Definition, where the strategy to mitigate/reduce, avoid or accept the risk is decided and defined.
- Risk Mitigation, where the mitigation measures (if a mitigation strategy is defined) are communicated to stakeholders and implemented.
- Remediation through Patch Management, which focuses on issuing and applying a patch/fix for the vulnerability on all affected assets, either custom-of-the-shelf products or built in-house.
- Remediation Monitoring aims to ensure that the vulnerability has been completely fixed. It involves also a scanning stage, during which the System managers of the systems that are still affected are warned and advised to patch the vulnerability.
- Lesson Learned, which aims at identifying lessons that may be learnt from the management of the vulnerability, once the risk is sufficiently reduced. This shall also encompass the identification of improvements in prevention, mitigation and remediation capabilities
- Closure, which defines the actions to close the management of a vulnerability.

3.3.7 OPS.Cfg – Secure Configuration Management

The configuration of an information system and its components has a direct impact on the security posture of the system. Changes to the configuration of an information system are often needed to stay up to date with changing business functions and services, and information security needs.
The Configuration Management (CM) Process comprises a collection of activities focused on establishing and maintaining the integrity of CIS and its components, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.

The *aim* of this process is to ensure CIS and its components are configured in a secure manner.

The *activities* employed by Secure Configuration Management Process are:

- Plan for security-focused configuration management
- Define and Implement configurations:

  - Develop, review, approve and implement secure baseline configurations for CIS and its components. The baseline configurations represent the most secure state consistent with operational requirements and constraints;
  - Consider security risks in approving the initial configuration, like risks posed by default configurations.
  - Identify and record configurations that impact the security posture of the CIS;
- Control configuration changes by analyzing their security implications and performing changes to configurations through Change Management.
- Monitor deviations of CIS and its components from the approved secure baseline configurations. Solve deviations.

3.4 [CHK] – IT Security Compliance – Review implementation of security processes

Applicable references	
Standards	Compliance (3602, new under development)
Guidelines	
Services	HR.DS3: IT Security inspections
External	NIST SP800-53 (Security and Privacy Controls for Federal Information Systems and Organisations) NIST SP800-64 (Consideration in the System Development Life Cycle) ISO 27001 (Information Security Management System – Requirements)

The objective of IT Security Compliance is to ensure that security is implemented and operated in accordance with CIS requirements.

There are two processes that make-up the security review:

3.4.1 CHK.Tec – Technical Security Review

Similar to the DEV.Tst Security Testing process from the DEV process, this process *aims* to discover security shortcomings in the [OPS] process, so they can be mitigated. As opposed to the preceding process, this process tests the actual security of the system. Some vulnerabilities cannot be found in the DEV process because the attack techniques are invented after the system has entered into operation.

The *activities* which make up this process are:

- Vulnerability scanning, the largely automated process of looking for vulnerabilities by attempting to execute a battery of relatively simple known attacks;
- Fuzzing, the largely automated process of fault injection through providing the system partly random input data and monitoring it for malfunction, followed by human analysis of the malfunctions;
- Penetration tests, the process of hired human analysts looking for vulnerabilities by attempting to execute attacks that are above the abilities of vulnerability scanners and rewarded based on effort, not results;
- Bug bounties, a variant of penetration testing with a looser contractual framework with the external testers, in which they are rewarded only for being the first to report a vulnerability;
- Responsible disclosure, the process of interacting with opportunistic external security researchers who report security vulnerabilities in exchange for recognition by the organization.

The deliverables of this process are vulnerability reports to guide the implementation of mitigating controls against them, which must then be implemented as part of the ‘OPS.Mgt – Operation and management of Security Measures’ Process.

3.4.2 CHK.Cpl – Compliance Security review

The aim of Compliance Security Review is to verify if the system complies with applicable information security requirements defined by the European Commission or by applicable

regulation, as identified in activity RM.SSC System Security Characterization. These requirements have been translated into specific security requirements during the RM process: as such, Compliance Security Review tests the success of implementing the planned controls, rather than the security of the system.

The *activities* in this process consists of:

- Independent review, carried out after major changes or with a given periodicity, meant to attest that the information security controls with which the CIS must comply are operating effectively and performed by a neutral, trustworthy party;
- Compliance audit meant to verify to what extent the security controls and policies are being followed.

3.5 [EOL] – Secure IT system decommissioning process – Securely Retire the CIS to its End-Of-Life

Applicable references	
Standards	Sanitisation of media (3602)
Guidelines	
Services	
External	NIST SP800-53 (Security and Privacy Controls for Federal Information Systems and Organisations) NIST SP800-64 (Consideration in the System Development Life Cycle) ISO 27001 (Information Security Management System – Requirements)

When information systems are transferred, become obsolete, or are no longer usable, it is important to ensure that Commission resources and assets are protected.
The EOL process of a system starts when the system ceases operation and continues indefinitely. In order to satisfy the system's security needs it is not sufficient to abandon the system as soon as it has stopped producing value, as this might expose to risk the assets it contains, as well as other systems it was interacting with during the [OPS] process.

This is why the security requirements must address the actions to be taken during the decommissioning of the system.

The decommissioning activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future, if necessary. Particular emphasis is given to proper preservation of the data processed by the system so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access.

3.5.1 EOL.P.D&T Planning for Disposal/ Transition of CIS

The *aim* of this process is to ensure proper decommission of CIS, by identifying the necessary steps, decisions, and milestones needed to properly close down, transition, or migrate a CIS or its information.

The main *activity* of this process is planning for disposal/transition of CIS. Planning for disposal of CIS and CIS components helps mitigating possible adverse outcomes like risks generated by disposed components which are still accessible/ in use.
Planning for disposal/transition of CIS components should also be performed throughout all phases of its life cycle, as hardware and software become obsolete or damaged. Similar planning and related activities (e.g. media sanitization, information preservation, etc.), should be performed when disposing for CIS components in any life-cycle phase.

3.5.2 EOL.SCP System Closure Preparation

The *aim* of this process is to implement the Disposal/ Transition Plan by performing the activities needed to prepare the System for closure.

These *activities* relate mostly to:

1) *Information preservation*
   When preserving information, organizations should consider the methods that will be required for retrieving information in the future.

2) *Media sanitization and Hardware and Software disposal*
   Media sanitization applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable.
   The organization that owns the CIS should approve, track, document and verify media sanitization and disposal.

3.5.3 EOL.SCl System Closure

At this point, the information system is formally shut down and disassembled.

ANNEX A.1: REFERENCES AND RELATED DOCUMENTS

ID	Reference or Related Document
[CD46/2017]	COMMISSION DECISION (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission
[IR46a/2017]	COMMISSION DECISION of 13.12.2017 laying down implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Decision 2017/46 on the security of communication and information systems in the Commission
[IR46b/2018]	COMMISSION DECISION of 6.04.2018 laying down implementing rules for Article 6 of Decision (EU, Euratom) 2017/46 on the security of communication and information systems in the European Commission.
[CD444/2015]	COMMISSION DECISION (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information
[CD443/2015]	COMMISSION DECISION (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission
[GDPR]	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[IDPR]	REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC
[R45/2001]	REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
NIST.SP.800-53 r4	NIST Special Publication no 800-53, rev.4 - Security and Privacy Controls for Federal Information Systems and Organizations
NIST.SP.800-64 r2	NIST Special Publication no 800-64, rev.2 - Security Considerations in the System Development Life Cycle
ISO27002 2ED	ISO/IEC 27002:2013 (2nd Edition) – Information technology - Security techniques - Code of practice for information security controls
BSIMM v9	'Building Security in Maturity Model' Framework. The BSIMM project is a de facto standard for assessing (and then improving) software security initiatives.

ITSec Portal	Portal: IT Security Policy, Standards, Guidelines and Technical specifications

ANNEX A.2: DEFINITIONS

Asset	An asset is anything that has value to the organization and which, therefore, requires protection. Two kinds of assets can be distinguished: - the Primary Asset (business processes and activities, information); - the Supporting Assets on which the Primary elements of the scope rely (hardware, software, network, personnel, site, organisation's structure). [ISO 27005:2018]
Authentication	Provision of assurance that a claimed characteristic of an entity is correct. [ISO 27000:2018]
Availability	Property of being accessible and usable on demand by an authorized entity. [ISO 27000:2018] The property of being accessible and usable upon request by an authorised entity. [CD46/2017]
Business continuity plan (BCP)	Documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption. [ISO 22301:2012] Documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical activities at an acceptable pre-defined level. [BS25999:2006]
Business impact analysis/assessment (BIA)	Another basis for the valuation of assets is the costs incurred due to the loss of confidentiality, integrity and availability as the result of an incident. Business Impact Assessment is considered here as the asset valuation based on estimates of the adverse business consequences that would result from security incidents with an assumed set of circumstances. [ISO 27005:2018]
Communication and information system (CIS)	Any system enabling the handling of information in electronic form, including all assets required for its operation, as well as infrastructure, organisation, personnel and information resources. This definition includes business applications, shared IT services, outsourced systems, and end-user devices. [CD46/2017]
Compliance	Adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies. [ISACA Cybersecurity Fundamentals Glossary]
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO 27000:2018] The property that information is not disclosed to unauthorised individuals, entities or processes. [CD46/2017]
Control	Measure that is modifying risk. Controls include any process, policy, device, practice, or other actions which modify risk. [ISO 27000:2018]
Data owner	The individual responsible for ensuring the protection and use of a specific data set handled by a CIS. [CD46/2017]
Information security	Preservation of confidentiality, integrity and availability of information. [ISO 27000:2018]

Information Systems	Set of applications, services, information technology assets, or other information-handling components. [ISO 27000:2018]
Integrity	Property of accuracy and completeness. [ISO 27000:2018] The property of safeguarding the accuracy and completeness of assets and information. [CD46/2017]
IT Security	Preservation of confidentiality, integrity and availability of CISs and the data sets that they process. [CD46/2017]
IT Security Incident	Event that could adversely affect the confidentiality, integrity or availability of a CIS. [CD46/2017]

ANNEX A.3: ACRONYMS

For the purpose of this document, the following acronyms have been used:

S²LC/ S2LC	The Life-Cycle of an IT System, comprising both, SDLC (System Development Life-Cycle) and SOLC (System Operations Life-Cycle)
CIS	Communication and information system
DG	Directorate General
EC	European Commission
GDPR	European Data Protection Regulation
ITS	Information Technology Security
ITSRM²	Information Technology Risk Management Methodology
LISO	Local Informatics Security Officer
SSO	System Security Officer
NIST	The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce – a science laboratory

ANNEX A.4: SYSTEM SECURITY PASSPORT

The following list can be used as a "Security Passport" for systems to follow their status and evolution by "applying visa" where the system passed the processes.

	Did your system passed the following process?	**Status (1)**	**When? (2)**
RM.SSC	System Security Characterisation		
RM.PA	Primary Assets		
RM.Mdl	System Model		
RM.Ast	Risk Assessment		
RM.Trt	Risk Treatment		
RM.A&C	Risk Acceptance and Communication		
DEV.Mgt	Secure Development Management		
DEV.Out	Secure outsourcing		
DEV.AA	Analyse the Architecture		
DEV.CR	Review the Code		
DEV.ST	Test the Security		
DEV.Dlv	Delivery to Operations		
DEV.Env	Secure development environment		
OPS.Mgt	Operation and management of Security Measures		
OPS.Mon	Security monitoring		
OPS.IM	Information Security Incident Management		
OPS.Spl	Supplier management		
OPS.CM	Change management		
OPS.VM	Vulnerability Management		
OPS.Cfg	Secure Configuration Management		
CHK.Tec	Technical Security Review		
CHK.Cpl	Compliance Security review		
EOL.P.D&T	Planning for Disposal/ Transition of CIS		
EOL.SCP	System Closure Preparation		
EOL.SCl	System Closure		

(1) Status:

- *a. Performed (process has been performed)*
- *b. Ongoing (process is ongoing)*
- *c. Planned (performing process has been planned)*
- *d. N/A (process is not applicable)*

(2) When?: specify the date if/when the process has been performed