DG DIGIT
Unit S1 – IT Security Policy

Description of the methodology

IT Security Risk Management Methodology v1.2

Date: 11/08/2020
Doc. Version : v1.2 r19

Document Control Information

Settings	Value
Document Title:	IT Security Risk Management Methodology v1.2
Project Title:	IT Security Risk Management Methodology v1.2
Programme Name:	IT Security Risk Management Programme
Document Author:	Joël HUBIN
Programme Owner (PgO):	Grzegorz MINCZAKIEWICZ
Programme Business Manager (PgBM):	Spyros SARIGIANNIDIS
Programme Manager (PgM):	Liliana MUSETAN
Doc. Version:	v1.2 r19
Sensitivity:	Internal
Date:	11/08/2020

Document Approver(s) and Reviewer(s):

NOTE: All Approvers are required. Records of each approver must be maintained. All Reviewers in the list are considered required unless explicitly listed as Optional.

Name	Role	Action	Date
Grzegorz MINCZAKIEWICZ	PgO	*Approve*	06/08/2020

Document history:

The Document Author is authorised to make the following types of changes to the document without requiring that the document be re-approved:

- Editorial, formatting, and spelling
- Clarification

To request a change to this document, contact the Document Author or Owner.

Changes to this document are summarised in the following table in reverse chronological order (latest version first).

Revision	Date	Created by	Description (*of Changes*)
			Changes - catalogue of measures
11	30/06/2020	JH	Review L. Musetan Added mapping for classification (Annex. B.1c)
12	02/07/2020	JH	Styles and cleaning
13	13/07/2020	LM	Headings, cross-references, list of figures and tables
14-16	27-31/7/2020	JH	Adding external review from DIGIT.B, SG, RTD, JRC, DIGIT cLISO, COMP
17-18	07/08/2020	JH	Review G. Minczakievicz and cleaning
19	11/08/2020	LM	Formating pages, doc location

Configuration Management: Document Location

The latest version of this controlled document is stored in:

https://webgate.ec.europa.eu/fpfis/wikis/display/ITSRM2/The+ITSRM+Methodology

Table of Contents

1 INTRODUCTION

Every Communication and Information System (CIS) is exposed to IT security threats, giving rise to IT Security Risks. As any other organisation, the European Commission (EC) must ensure the appropriate IT Security of its CIS. It is widely recognised that IT Security Risk Management is the main means to provide appropriate security by prioritising risks, focusing on main values, and helping to identify the most suitable Security Measures.

This is emphasised in the COMMISSION DECISION (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission which states: "*IT security shall be based on a risk management process. This process shall aim at determining the levels of IT security risks and defining Security Measures to reduce such risks to an appropriate level and at a proportionate cost*" ([CD46/2017][1] Art.3 §4).

In this context, DIGIT proposes the IT Security Risk Management (ITSRM) Methodology to complement the efforts of the EC for the "*protection of the information systems as an integral part of the Functioning of the Commission from IT security incidents that can have a serious impact on the Commission's operations as well as on third parties, including individuals, businesses and Member States*" ([CD46/2017] Recital, point (1)).

The first version of the methodology ITSRM[2] v1.0 has been published in March 2018. Meanwhile, some concepts, such as the sharing of Services, have been clarified and documented. Some others have been added, notably to incorporate the protection of Personal Data. A list of changes to the present version ITSRM Methodology v1.2 from August 2020 are detailed in Annex A.4.

1.1 How to read this document

In the first chapter, preliminary concepts will be defined and the approach used to build the ITSRM Methodology will be presented.

The following chapters will describe each process of the ITSRM Methodology, one by one with grouped per sub-sections:

Key concepts

This section will highlight the concept required to understand the description of the process.

Process description

In a standard way by providing:

- process ID (identification of the process)
- name
- purpose
- outcomes

Inputs and Outputs

This section will describe the inputs and outputs of the process.

Tasks

The tasks proposed to produce expected outcomes will be further detailed and each task will be linked to IT Security roles via a RASCI Matrix - an expanded version of Responsibility Assignment Matrix.

The key IT security roles to be involved in the execution of each task/process are in line with those included in the [CD46/2017]:

- Head of Commission Department (HoD): Head of the Commission Directorate-General or service, or any Cabinet of a Member of the Commission owning the Target System;

[1] COMMISSION DECISION (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission

- System Owner (SO): individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and decommissioning of a CIS;
- Data Owner (DO): individual responsible for ensuring the protection and use of a specific Data Set handled by a CIS;
- Local Informatics Security Officer (LISO): officer responsible for the IT security liaison for a Commission department;
- Data Protection Coordinator (DPC): role responsible for Data protection issues regarding the regulation applied in the Commission;
- IT Staff: IT-related personnel in charge of development and/or operation of the CIS;
- Security Risk Manager (SRM): the person performing the Risk Management.

The RASCI values and their description are presented in the Table 1-1: RASCI values:

RASCI value		Description
R	Responsible	Has the obligation to act and take decisions to achieve required outcomes. Does the work. Others can be asked to assist in a supporting role.
R(D)	Responsible	Responsible by delegation
A	Accountable	An accountable role is answerable for actions, decisions and performance. Ultimately answerable for the correct and thorough completion of the work. There is just one accountable person.
S	Supports	People that actively support the work developed by the responsible roles.
C	Consulted	Roles used to complete, complement or validate the information resulting from each process.
I	Informed	Those informed (kept up-to-date) of the results obtained from the execution of the methodology.

Table 1-1: RASCI values

1.2 Key definitions

As defined in [CD46/2017], IT Security means the preservation of confidentiality, integrity and availability of CISs (Communication and Information Systems) and the datasets that they process.

Confidentiality, Integrity and Availability of Data Sets are the three main properties, called Security Dimensions in this methodology, that need to be protected in the context of IT Security as defined in [CD46/2017]:

- Confidentiality: *the property that information is not disclosed to unauthorised individuals, entities or processes*;
- Integrity: *the property of safeguarding the accuracy and completeness of assets and information*;
- Availability: *the property of being accessible and usable upon request by an authorised entity*.

The definitions of the concepts used in this methodology are included in the annex A.2. Most of them are aligned with the terminology used in recognised standards and methodologies such as ISO, EBIOS, Magerit or NIST. Nevertheless, the following terms have been defined specifically for this methodology to simplify writing and ease reading:

- the Target System refers to the specific CIS on which the Risk Management is performed following the methodology;
- the IT Security Risk Manager, shorten to Security Risk Manager (SRM) in the text, is the person actually performing the Risk Management.

1.3 ITSRM Methodology approach

The ITSRM Methodology v1.2 has been developed, like the previous version ITSRM² v1.0, based on the ISO 27005 standard:

(1) the pragmatic definition of an IT Security Risk that can be derived from the standard (in *italic* below):

- *An IT Security Risk is a combination of the CONSEQUENCE of an IT Security Incident and the associated LIKELIHOOD of its occurrence*;

(2) the definition of the (main) Risk Management processes:

- Context Establishment that describes *the scope and boundaries, and the organisation for the Risk Management Process*
- Risk Assessment that is the *overall process of Risk Identification, Risk Analysis and Risk Evaluation*; and
- Risk Treatment that is the *process to modify risks* up to an acceptable level.

While the ISO 27005 standard defines these processes and their expected outcomes, proposes different ways of reaching these outcomes with different examples for scales, catalogues and formulas, it does not go into the details and does not mandate any.

Like other Risk Management Methodologies, the ITSRM Methodology proposes practical choices of implementation of these processes by providing:

- detailed formulas to assess the RISK LEVEL and the Residual RISK LEVEL;
- actionable tasks and methods per Risk Management sub-process to achieve their respective outcomes, mainly building and assessing the different components of the risk;
- scales to be used corporate wide aiming to achieve comparable results in all DG's;
- catalogues to facilitate the processes and to be used corporate wide to be able to consolidate results at EC level.

1.3.1 Mapping ITSRM Methodology processes to ISO 27005 standard

The mapping between Risk Management processes as defined in ISO 27005 and their implementation as developed in the ITSRM Methodology is depicted in the Figure 1-1: Mapping between ISO 27005 and ITSRM Methodology processes.

As this version of the ITSRM Methodology focusses on IT Security Risk Management, implementation of the three following processes is not detailed:

- Risk Acceptance is not present as such, but it is included as ending step in the Risk Treatment of Residual Risks.
- Risk Communication and Consultation is included in the reporting and communication on the outcomes of the processes.
- Risk Monitoring and Review is part of the Risk Management processes at governance level.

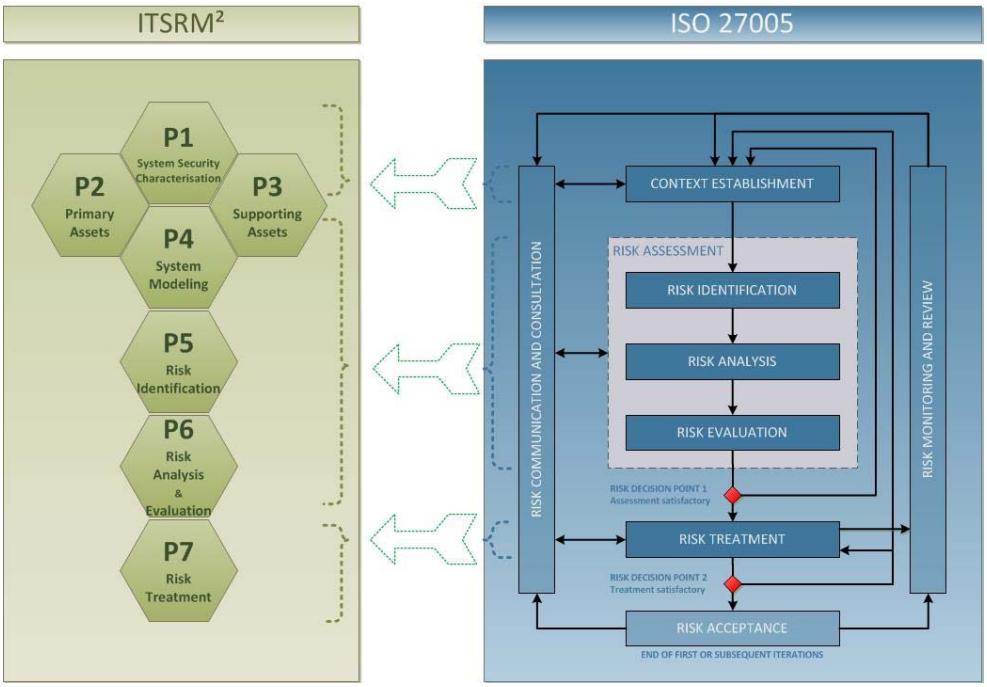


Figure 1-1: Mapping between ISO 27005 and ITSRM Methodology processes

Concerning the other ISO 27005 processes:

- Context Establishment is mainly implemented in P1 (System Security Characterisation).
- Risk Identification is split into 4 pragmatic sub-processes:
  - P2 (Primary Asset) dealing with Primary Assets;
  - P3 (Supporting Assets) dealing with Supporting Assets;
  - P4 (System Modelling) grouping Primary Assets and Supporting Assets to build a model of the system;
  - P5 (Risk Identification) identifying risks by performing a threat analysis based on the model.
- Risk Analysis and Risk Evaluation processes are grouped into one process, P6 (Risk Analysis and Evaluation), which calculates Residual RISK LEVELS (risk analysis) and sorts them by level (risk evaluation), to ease acceptance decision.
- Risk Treatment process is implemented in P7 (Risk Treatment).

A Risk Study is defined as the process and results of performing P1 (Context Establishment), P2-P6 (Risk Assessment) and P7 (Risk Treatment).

1.3.2 The risk formula

The risk formula defines the actual implementation of a Risk and its Level. Based on the definition of an IT Security Risk above, a Risk Level (RL) will be calculated and represented in two possible ways based on the assessment of the LIKELIHOOD (LH) and of the CONSEQUENCE (CSQ) of an IT Security Incident, as depicted in Figure 1-2: Risk Matrix:

1. the values for LIKELIHOOD and CONSEQUENCE are used as coordinates (LH , CSQ) to position the risk on a Risk Matrix (also known as Risk Heat Map); and
2. the risk is calculated as the product of the LIKELIHOOD and the CONSEQUENCE (LH x CSQ).

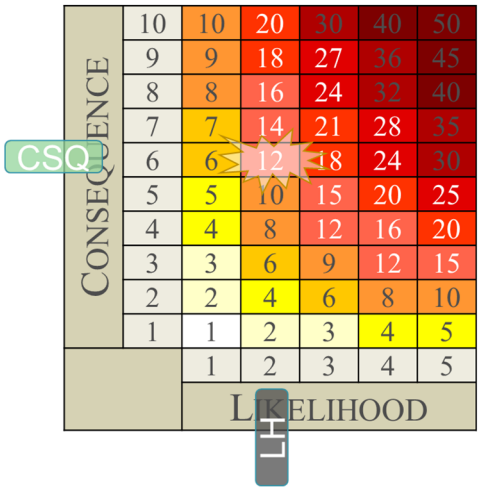


Figure 1-2: Risk Matrix

This is called Inherent RISK LEVEL i.e. the RISK LEVEL considering that no security measure is applied that could reduce it.

To assess the LIKELIHOOD and the CONSEQUENCES, the ITSRM Methodology considers that an IT Security Incident is caused by "an IT Security Threat to an asset which can harm one of its Security Dimensions (Confidentiality, Integrity, Availability).

Assets are further divided into two categories:

- Primary Assets (mainly Data Sets and Functions), under the control of Business, and
- Supporting Assets (mainly hardware, software, people, locations and services used to store, transmit and process the Primary Assets), under the control of IT.

As, in practice, threats occur on the Supporting Asset, we identify an IT Security Risk as a Risk Scenario composed of an IT Security Threat occurring on a Supporting Asset and harming a Security Dimension (confidentiality, integrity, availability) of a Primary Asset which it processes.

Following the Risk formula, we can further define and assess:

- Asset Value: the maximum Impact (Business or Data Protection) in case of loss of a Security Dimensions (confidentiality, integrity, availability) of a Primary Asset; this is also known as the Security Need;
- FREQUENCY: the statistical frequency of a non-intentional threat;
- EASINESS: the easiness to commit a given intentional threat;
- POWER: the capacity of an adversary that could be interested to commit a threat on a given Primary Asset;
- INTEREST: the level of INTEREST of an adversary to commit a threat on a given Primary Asset.

With those definitions, we consider:

- the CONSEQUENCE of an IT Security Event is proportional to the value of the Primary Asset which is harmed;
- the LIKELIHOOD of an IT Security Event is proportional to the FREQUENCY of a non-intentional threat, and to the EASINESS, POWER and INTEREST for an intentional threat.

The ITSRM Methodology consequently proposes the following formulas to assess the LIKELIHOOD and CONSEQUENCE of risks:

CSQ	= Asset Value	
LH	= FREQUENCY	(for non-intentional threats)
	= (EASINESS + POWER + INTEREST) / 3	(for intentional threats)

A Residual Risk (RR) is defined as the Risk after treatment.

To assess the Residual Risk Level (RRL), we consider that each Security Measure (SMi) has a Mitigation Factor (MF) for a given threat (MF(SMi)), i.e. a percentage of reduction of the associate RISK LEVEL, and we apply this factor to the RISK LEVEL for the n Security Measures that are chosen to mitigate the risk:

$$RRL = RL * (1 - MF(SM1)) * \dots * (1 - MF(SMn))$$

With this Risk reduction formula, we have all the formulas and parameters that we need for Risk Management.

Each Risk Management sub-process will be refined in next sections and will explain how it is proposed to assess the different parameters of the global Risk formula.

1.3.3 The ITSRM Methodology processes

The ITSRM Methodology processes are described by their main outputs and their sequence of execution (see schema below):

- Each process, individually, is defined to record and provide information useful for the security of the Target System but can be useful per se. For example, it builds an inventory of primary assets processed in a Commission department.
- Processes are interlinked, the output of one process being usually the input for next one.
- The global Risk Management process is iterative and produces incremental outputs, meaning that the complete cycle (P1-P7) can be performed with basic inputs, providing an initial list of Residual Risks corresponding to an initial list of Security Measures. Additional cycles may be initiated by entering additional information into any process and perform following processes. This provides results in an "agile" way.
- The Risk Treatment process is the heart of the main iteration as the Security Risk Manager (SRM) will cycle on (Risk Treatment – Risk Analysis & Evaluation) until Residual Risks are acceptable for System Owner.
- The model of the system is pivotal in the Methodology: the more detailed the model is, the more detailed the Risk Management can be. One can perform a high-level Risk Management on a high-level model at first and then produce results that are more detailed by enriching iteratively the model of the system.

1.3.4 Catalogues

The catalogues provide guidance to the Security Risk Manager (SRM) in the execution of the tasks foreseen in each process. They are structured in levels to allow the selection of generic or specific elements and the possibility of further detailing the information that identified the elements required in each process. The structure of the catalogues allows filtering the information provided to limit the selection of applicable information and provides guidance to the Security Risk Manager (SRM) towards the correct option. For example, this approach will limit the type of relevant threats regarding the type of Supporting Assets.

The catalogues provided with this methodology include:

- Constraint types (Annex C.1)
- Asset types (Annex C.3)
- Potential Adversaries types (Annex C.2)
- Threats (Annex C.4)
- Security Measures (Annex C.5)

1.3.5 Scales

Scales support the understanding of the levels used to value some concepts of the risk management, such as the impact on an asset. These levels are represented qualitatively (e.g. LOW/MEDIUM/HIGH) and with a semi-quantitative value (e.g. 1/2/3).

- Impact (Business or Data Protection) per Impact type
- LIKELIHOOD
- FREQUENCY (of a non-intentional Threat)
- EASINESS (to perform an intentional Threat)
- POWER (of a Potential Adversary)
- INTEREST (of a Potential Adversary to threaten an asset)
- Risk level

2 PROCESS 1 – SYSTEM SECURITY CHARACTERISATION

2.1 Key concepts

There are no key concepts for this simple process.

2.2 Process description

Process ID	RM.P1-SSC
Name	P1 – System Security Characterisation
Purpose	The System Security Characterisation process gathers initial information concerning the Target System and its context which is required or helpful to proceed further with the Risk Management
Outcomes	(1) The Target System is identified and described (high level) (2) Responsible and contact point for the security roles for the Target System are identified (3) The organisation owning the Target System is identified and described (4) Main constraints and requirements on the Target System having a possible effect on its security are identified (5) Mandatory Security Measures, mandated by constraints to the system, are identified. (6) Risk Acceptance Criteria(s) is/are recorded, if defined

2.3 Inputs and Outputs

Inputs	
Unstructured	Public and internal resources related to the organisation and to the Target System (organisation website, intranet, system documentation, …)
Unstructured	Interviews with the different security actors
IN01.01	Catalogue of Constraint types (Annex C1)
Outputs	
OUT01.01	System Description
OUT01.02	Security Roles
OUT01.03	Organisation Description
OUT01.04	Constraints Identification
OUT01.05	Security Measures Register: The list of Security Measures selected for the Risk Management. At this stage, mandatory measures, i.e. measures coming from a constraint (legal constraint, mandatory baseline, …), can be added. Minimum content recommended: • Security Measure ID: Identification of the Security Measure. • Target of the measure**:** Either 'Organisation', 'System', or the Supporting Asset ID (identification of the Supporting Asset on which the measure will be applied/implemented to reduce the risk). • A flag (M): at this stage, the flag will be "M" specifying that the implementation of the Security Measure is mandated by a security-related constraint.
OUT01.06	Risk Acceptance Criteria A simple Risk Acceptance Criteria is recorded as a set of thresholds on the risk parameters (usually LIKELIHOOD, CONSEQUENCE and/or RISK LEVEL). A complex Risk Acceptance Criteria is recorded as free text.

2.4 Tasks

	SO	DO	LISO	DPC	SRM	IT Staff	HoD
P1 – System Security Characterisation							
System Description	R	-	S	C	R(D)	-	A
Identification of Security-related Roles	R	-	S	-	R(D)	-	A
Organisation Description	R	-	S	-	R(D)	-	A
Identification of Main Constraints	R	-	S	-	R(D)	-	A
Identification of Mandatory Security Measures	R	-	S	C	R(D)	-	A

2.4.1 System Description

The objective of this task is to identify and provide a high-level description of the Target System focussing on any relevant characteristics that may condition the security requirements that need to be addressed. This will include:

- the Target System name;
- a global description of its main purposes and Functions (in relation to the business objectives);
- a global description of the main information pieces it handles;
- a global description of its user population;
- a high-level architecture of the Target System (main components with business location).

The user population includes the units or specific user groups that use the Target System. Their identification will help to ensure that all relevant Data and Functions are considered in relation to the business activities covered by the different areas of the organisation. Typically these units will be directly related to the Data and Functions, managed and provided by Target System.

2.4.2 Identification of security-related roles

The persons nominated as responsible for the following security roles, as mainly defined in [CD46/2017], should be identified:

- System Owner (SO)
- Data Owner(s) (DO)
- Local Informatics Security Officer (LISO)
- Data Protection Coordinator (DPC)
- Security Risk Manager (SRM)

The persons in charge of the following operational roles, as defined in [IR46/2017], could also be identified:

- Project Manager (PM)
- System Manager (SM)
- System Security Officer (SSO)
- System Supplier (SS)
- IT Service Provider (ITSP)

It is also advisable to maintain pragmatic contact point(s) for these roles.

2.4.3 Organisation Description

The objective of this task is to identify and provide a high-level description of the organisation owner or stakeholder of the Target System providing:

- the name of the organisation and
- a brief description of its main business objectives.

The Security Risk Manager (SRM) can validate or complement this information consulting available public or internal information related with the organisation.

2.4.4 Identification of main constraints

The Target System can be subject to different constraints that can affect further Risk Management processes. This could be the case, for example, if the Target System is subject to a given regulation which mandates the implementation of a particular Security Measure.

The Security Risk Manager (SRM) should identify and register any constraint that could condition the security requirements, actions or any other relevant issues related with the Target System.

Annex C.1 contains a list of possible types of constraints to ease their identification.

The Security Risk Manager (SRM) should at least check if it is already known that the Target System will handle Personal Data as defined in applicable legislation ([GDPR][2], [IDPR][3]) or Classified Information as defined in [CD444/2015][4]:

- Personal Data according to the applicable Data Protection regulation, and Sensitive Personal Data ("special categories of personal data" or "personal data relating to criminal convictions and offences"). The latter usually includes personal information related to the following:
  a) racial or ethnic origin;
  b) political opinions;
  c) religious or philosophical beliefs;
  d) trade union membership;
  e) genetic data, biometric data for the purpose of uniquely identifying a natural person
  f) data concerning health;
  g) data concerning a natural person's sex life or sexual orientation;
  h) personal data relating to criminal convictions and offences.

If the Target System will process Personal Data, the Security Risk Manager (SRM) should consult the DPC of its DG. It is reminded that processing of personal data relating to criminal convictions and offences shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law [GDPR].

- Classified Information according to a Classification regulation, and its level of classification. For EU Classified Information (EUCI), this can be:
  a) RESTREINT UE/EU RESTRICTED
  b) CONFIDENTIEL UE/EU CONFIDENTIAL
  c) SECRET UE/EU SECRET
  d) TRES SECRET UE/EU TOP SECRET

If the Target System will process Classified Information, the Security Risk Manager (SRM) must immediately consult HR.DS before proceeding further.

2.4.5 Identification of Mandatory Security Measures

Usually, mandatory Security Measures are derived from legal, compliance or regulatory constraints, typically expressed in:

- security-related legal bases;
- Security Policies and Standards;
- Security baselines;

[2] [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)

[3] [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

[4] [CD444/2015] - COMMISSION DECISION (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information

- applicable legislation on processing of Personal Data;
- applicable legislation on processing of Classified Information.

The Security Risk Manager (SRM) should gather and analyse these artefacts to identify security measures they require to be implement in the target system. These mandatory measures should be added to the Registry of Measures and flagged as "Mandatory" for further treatment in following processes, notably in Risk Treatment.

2.4.6 Definition of the Risk Acceptance Criteria

During Risk Treatment (Process 7), the Security Risk Manager (SRM) will have to decide if the risk can be proposed for acceptance. Such decision is often based on a Risk Acceptance Criteria.

In theory, *risk acceptance criteria should be developed and specified* before risk assessment and treatment. As risk acceptance criteria often *depend on the organisation's policies, goals, objectives and the interests of stakeholders*, they could be specified at the level of the organisation.

But in practice, as explained in [ISO27005], *risk acceptance can be more complex than just determining whether or not a residual risk falls above or below a single threshold*. And it can even be impossible to have a generic criteria at the level of the organisation, fitting all its Departments, businesses and systems.

Risk acceptance criteria often depend on the organisation's policies, goals, objectives and the interests of stakeholders.

An organization should define its own scales for levels of risk acceptance. The following should be considered during development:

- *risk acceptance criteria may include multiple thresholds, with a desired target level of risk, but provision for senior managers to accept risks above this level under defined circumstances;*
- *risk acceptance criteria may be expressed as the ratio of estimated profit (or other business benefit) to the estimated risk;*
- *different risk acceptance criteria may apply to different classes of risk, e.g. risks that could result in noncompliance with regulations or laws may not be accepted, while acceptance of high risks may be allowed if this is specified as a contractual requirement;*
- *risk acceptance criteria may include requirements for future additional treatment, e.g. a risk may be accepted if there is approval and commitment to take action to reduce it to an acceptable level within a defined time period.*

Risk acceptance criteria may differ according to how long the risk is expected to exist, e.g. the risk may be associated with a temporary or short term activity.

Risk acceptance criteria should be set up considering the following:

- *Business criteria*
- *Legal and regulatory aspects*
- *Operations*
- *Technology*
- *Finance*
- *Social and humanitarian factors*

ITSRM Methodology proposes to record a Risk Acceptance Criteria in two possible ways.

A simple Risk Acceptance Criteria consists in 1, 2 or 3 values which will be considered as thresholds, possibly combined, for:

1. Maximum acceptable LIKELIHOOD of the risk (0-5);
2. Maximum acceptable CONSEQUENCE of the risk (0-10);
3. Maximum acceptable RISK LEVEL (0-50).

Based on such criteria, some decisions in the risk treatment can be somehow automated, eventually. For example, the Security Risk Manager (SRM) could automatically propose to retain all risks below these thresholds.
In the case of a complex Risk Acceptance Criteria, depending on several parameters as presented above, it is recorded as free text in this process. In this case, all decisions in the risk treatment have to be evaluated case by case.

3 PROCESS 2 – PRIMARY ASSETS ANALYSIS

3.1 Key concepts

- Asset: something worth protecting, either tangible or intangible.
- Primary asset: the Data Sets[5] or Data (for short) managed by the Target System and the Functions[6] provided by it.
- Primary Asset Container or Container (for short): in some circumstances, details about a Primary Asset processed by a CIS are not known in advance. The CIS is developed to handle such Primary Asset in a generic way, not knowing in advance exactly which Primary Asset it will be. This is the case for infrastructures: for example, a network, a file server or a database will handle Primary Assets for their users but their exact type is not known in advance. This is also the case when developing a CIS such as a Document Management System which will handle any "document" in a generic way, without knowing the exact type of document. Such generic Primary Assets are referred to as Primary Asset Container.
- Impact: adverse change to the level of business objectives achieved used to determine the Primary Asset value.
- Asset Value: value of the asset assessed in terms of the maximum Impact (Business or Data Protection) in case of loss of a Security Dimensions (confidentiality, integrity, availability); this is also known as the Security Need. Asset Value is a tuple with as many components as there are security dimensions envisaged, e.g. (C=2, I=3, A=4).
- System Value: by extension, the System Value is the maximum of the values of the assets processed therein for each of the Security Dimensions i.e. (Max(C), Max(I), Max(A)).
- Potential Adversary**:** Individual or group interested in provoking loss of Confidentiality, Integrity and/or Availability of any Primary Asset of the Target System Primary Assets.
- POWER of a Potential Adversary: its characterisation by its available capacity to perform a threat.
- INTEREST of a Potential Adversary: its characterisation by its willingness to use their capacity to threaten a given asset.
- Asset Attractiveness: the maximum combination of POWER and INTEREST for a Potential Adversary, for a given Primary Asset and Security Dimension.
- Data Subject: A data subject is any person whose personal data is being collected, held or processed.
- Personal data: any information relating to an identified or identifiable natural person ('data subject')

3.2 Process description

Process ID	RM.P2-PA
Name	P2 – Primary Assets
Purpose	The objective of the Primary Asset analysis process is to identify and describe the Data and Functions comprised in the system, to assess their business value, and to identify and assess Potential Adversaries.
Outcomes	(1) The Data and Functions in the system are identified and described. When they are Primary Asset Containers, they are flagged as such. When they are Personal Data, they are flagged as such. (2) Their respective owners are identified. (3) Their value, in terms of Confidentiality, Integrity and Availability, is assessed, or is stated as hypothesis in the case of Primary Asset Containers. (4) Their attractiveness is assessed, or is stated as hypothesis in the case of Primary Asset Containers. (5) The assessment of asset value is based on plausible and pertinent impact scenarios on different categories (impact on business, impact on data subject).

[5] Commission Decision 46/2017: A Data Set is a set of information which serves a specific business process or activity of the Commission.

[6] Commission Decision 46/2017: 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.

	(6) The assessment of attractiveness is based on the identification of Potential Adversaries and the assessment of their POWER and INTEREST.

3.3 Inputs and Outputs

Inputs	
OUT01.01	P1- SSC results The results obtained from the System Security Characterisation process help to identify the Primary Assets within the Target System boundaries.
IN02.01	Impact (Business or Data Protection) Scale (Annex B.1) This table comprises a list of relevant impact types for the EC. It can help the Security Risk Manager (SRM) Data and System owners to determine the impact level of the Primary Assets according the potential business consequences in case of harm or loss of a Primary Asset.
IN02.02	Potential Adversaries Catalogue (Annex C.2) List of Potential Adversaries with a potential Interest in harming Primary Assets. The information provided includes a description of these Potential Adversaries and a POWER value proposed for each of them.
IN02.03	Interest level Scale (Annex B.2) This table includes a definition of the level of INTEREST of the Potential Adversaries in the Primary Assets.
Outputs	
OUT02.01	Primary Asset inventory This inventory includes the identification and description of the Data managed and the Functions provided by the Target System. Minimum content required for the Primary Asset inventory: • PA ID: identification of the Primary Asset • Name: name used in the context of the EC to identify the Primary Asset • Type: Identify if the Primary Assets is a Data Set or a Function • Container flag: flag indicating if the Primary Asset is a container or not • Personal Data flag: flag indicating if the Primary Asset contains a Personal Data or not • Description: Provide a brief description of the main characteristics of the Primary Assets • Owner: Identify the person (name, surname and contact information) or entity (Unit, Directorate or Directorate-General) owner of the Primary Asset. For a Data Set, it is its Data Owner. For functions, it can be globally the System Owner, or it could be, if known, its Business Manager as defined in PM² [7]. • Security dimension: security feature affected by the impact (confidentiality, integrity or availability) in relation to the Primary Asset; • Asset Value**:** assessment or statement of the value of the asset in terms of Impact (Business or Data Protection) Level in case of loss of Confidentiality, Integrity and Availability • Asset Attractiveness: the maximum combination of POWER and INTEREST for Potential Adversaries, for a given Primary Asset and Security Dimension
OUT02.02	Impact scenarios This list includes the Impact Scenarios that are used to assess and justify Asset Value of each Primary Asset in each Security Dimension from a business and data subject perspective. Impact Scenarios are pertinent in case of Asset Valuation by performing an Impact Assessment (IA), when the Primary Asset is not a container. Minimum content recommended to build Impact Scenarios: • Scenario ID: Identification of the scenario • Primary Asset ID: identification of the Primary Asset • Security dimension: Security Dimension affected at the end of the scenario (confidentiality, integrity or availability) in relation to the Primary Asset;

[7] PM² - Project Management Methodology – Guide 3.0 (2018)

	• Description: textual description of plausible scenario explaining what could happen after a loss of Security Dimension, and its effects at the end on the Primary Asset; • Impact type: type of impact caused to the organisation, such as financial, political, operational, etc. • Description of Consequences: Effects of the impact on the organisation. For example, the effects of the impact type "damage to organisations image and reputation" includes "negligible damage to image and reputation" (Level 1) to "More than serious, Europe wide or worldwide negative publicity" (Level 7). • Impact level: Level of damage that the organisation could suffer, corresponding to the description of consequences chosen (effect of the impact). This is translated to the scale levels from 0 to 10.
OUT02.03	Interest scenarios This list includes the Interest Scenarios that are used to identify Potential Adversaries and to assess and justify their POWER and INTEREST for each Primary Asset in each Security Dimension. Potential Adversaries can be interested by the disclosure, modification or unavailability of Organisation's Primary Assets. These are pertinent when the Primary Asset is not a container. The content that will be represented in each interest scenario includes; • Scenario ID: Identification of the scenario • Primary Asset ID: identification of the Primary Asset • Security dimension: security dimension interesting the Potential Adversary (confidentiality, integrity or availability) in relation to the Primary Asset; • Potential Adversaries**:** individuals or groups with interests on the organisations Primary Asset; • Description: textual description of plausible scenario explaining what could happen after threatening a Security Dimension, and the gain that the Potential Adversary could expect at the end; • POWER Level: Level of Power of the identified adversaries regarding the proposals provided in the *Catalogue of Potential Adversaries* (Annex C.2); if the Security Risk Manager (SRM) uses the Potential Adversary catalogue for the identification of the Potential Adversaries s/he will obtain directly from the catalogue the POWER values assigned to each adversary; if the Potential Adversaries is obtained from the organisation past experience or knowledge, then the Security Risk Manager (SRM) needs to assign their respective levels of POWER manually; • INTEREST Level**:** Level of INTEREST of the identified adversaries regarding the definitions provided in the *Interest Level Scale* (Annex B.2); the INTEREST of a Potential Adversary is in relation to the benefit that can be obtained from threatening the Security Dimension of the Asset.

3.4 Tasks

	SO	DO	LISO	DPC	SRM	IT Staff	HoD
P2 – Primary Assets							
Primary Asset Identification	R	S	C	C	R(D)	S	A
Asset Valuation	R	S	C	C	R(D)	-	A
Primary Asset Attractiveness Valuation	R	S	C	C	R(D)	-	A

3.4.1 Primary Asset Identification

The objective of this task is to identify the Data and Functions related with the Target System considered assets due to their importance for the organisation to achieve their business objectives.

The identification of the related Data and Functions will be aligned with the definitions provided in this methodology. Primary Assets that are Containers should be identified as such.

Examples of Data are user databases, payroll files, strategic plans, growth forecasts, Commission or system documentation, contracts, user manuals, training material, operational or support procedures, guidelines, documents containing important results of the Commission's business, continuity plans, or fall-back arrangements.

Examples of functions are generating the payroll, viewing a scorecard, processing an invoice, etc.

For the description of the Primary Assets, the Security Risk Manager (SRM) should focus on the identification of any characteristics that could condition the security requirements that need to be addressed in respect to the identified Data and Functions.

The Security Risk Manager (SRM) should start by consulting the System Owner and Data Owners to complete this task.

3.4.2 Asset Valuation

The objective of this task is to determine the Primary Asset value from a Business and a Data Protection perspective. This objective can be achieved through one of the following methods.

3.4.2.1 Option 1: By re-use of previous valuation

When valuating Primary Assets that have already been valuated, the Security Risk Manager (SRM) can simply reuse the value obtained from experience or from previous Impact Assessments, after adaptation to the ITSRM Methodology scale if needed.

3.4.2.2 Option 2: By estimation based on Impact (Business or Data Protection) scale

The Security Risk Manager (SRM) can estimate with Data Owners, based on their knowledge and experience, where the business value of the asset best fit in the Impact (Business or Data Protection) Scale provided in Annex B.1.

3.4.2.3 Option 3: By hypothesis

When it is not known in advance which Data will be processed and which Functions will be executed by the Target System, it is impossible to assess their value.

This is the case of Primary Asset Containers, when the Target System is an infrastructure, a middleware or a generic service (e.g. a file server, a document management system, a Database).

In this case, the value of the asset can only be decided and taken as an hypothesis to build the system, or a constraint to its use: the Risk Management of the Target System is done based on these hypothesis and it will consequently be developed to handle Data valued up to this stated maximum level.

3.4.2.4 Option 4: By formal Impact Assessment (IA)

This is the recommended option as it builds the valuation on factual reasoning and documents the justification of the selected Primary Asset values. The Impact Assessment (IA) is a technique to estimate the Primary Asset values based on the potential consequences for the organisation in case of a loss of the confidentiality, integrity and/or availability of the identified Primary Assets. It will be exemplified and justified by building plausible scenarios fitting the context of the organisation regarding the Data and Functions identified.

To develop such IA the Security Risk Manager (SRM) will perform the following steps:

Step 1: Contact the Primary Asset owners
Contact the people identified as the Data and Function owners in the previous task to ensure a correct understanding of the Primary Asset values from a business perspective.

The Security Risk Manager (SRM) and the Primary Asset owners will review the Data and Functions identified in this process to build and describe the scenarios required to complete the next step.

Step 2: Build and describe impact scenarios

The aim of this step is to build the impact scenarios from a Business and Data Protection perspective and then, from the information provided, identify the most relevant types of impact.

To complete this step the Security Risk Manager (SRM) will develop a brainstorming session with the stakeholders that are the most knowledgeable about the business supported by the Target System, by its Data Sets and Functions (e.g. System and Data owners, Business Managers, experienced users or future users of the Target System). This is to ensure most relevant potential consequences are related to the Primary Assets and included in the description of each scenario, considering the business objectives of the Organisation.

Once description of the scenario is registered, the Security Risk Manager (SRM) will focus on the identification of the consequences, related to the confidentiality, integrity and availability of the Primary Asset. To complete this approach, the Security Risk Manager (SRM) will analyse each scenario considering:

- Confidentiality: Determines the Impact (Business or Data Protection) by assessing the extent of the harm to the organisation and/or Data Subject that would result from an unauthorised disclosure of the Primary Asset.
- Integrity: Determines the Impact (Business or Data Protection) by assessing the extent of the harm to the organisation and/or Data Subject that would result from a corruption or unauthorised modification of the Primary Asset.
- Availability: Determines the Impact (Business or Data Protection) by assessing the consequences of a loss of accessibility to the Primary Asset. The availability of Data should be understood as being accessible to its users timely and in a user-friendly way.

NOTE**:** The impact of lack of availability (outage) of a Primary Asset usually depends on the duration of the outage. For example, if the unavailability of an asset is just a few seconds, impact can be negligible, if it is unavailable for a few minutes, the impact could be very low, while if the asset is unavailable for a day the impact would be unacceptable.
As depicted in Figure 3-1: Real and modelled impact curve for availability, impact of unavailability of an asset usually follows an S-curve in function of the duration of the unavailability. The curve starts from zero when it does not suffer from any unavailability. Impact then increases slowly with duration of outage. At a certain duration of unavailability, impact starts increasing quickly. It then stabilises at a certain ceiling, as after a certain unavailability duration, the impact cannot really grow anymore.
Typically, the duration of unavailability when the S-curve accelerates, its inflection point, is the duration after which the impact would be considered unacceptable. In Business Continuity, this duration is called Maximum Tolerable Period of Disruption (MTPD).

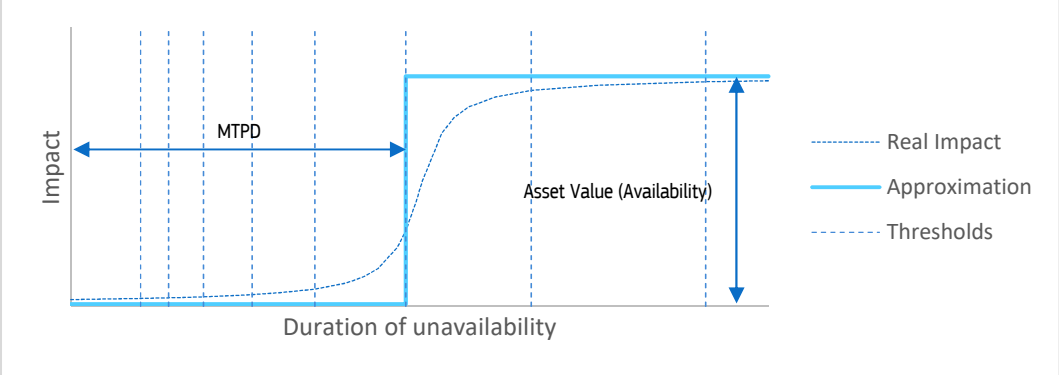


Figure 3-1: Real and modelled impact curve for availability

It is very important to identify the Maximum Tolerable Period of Disruption (MTPD) of any Primary Asset as this will determine the appropriate type of security measure that will need to be implemented in order to protect its availability. For example, if the MTPD of a data set is 10 seconds, its protection will require fail-over techniques, while a data set that can be unavailable during several hours can be protected by backup and recovery techniques.

To determine the MTPD, the Security Risk Manager (SRM), in consultation with the System Owner and Data Owner, will choose from among several fixed thresholds the closest one to the inflection point of the S-shape. The Security Risk Manager (SRM) can use any time slots to approximate the MTPD. This Methodology

proposes to use timeslots defined in Table 3-1 – Thresholds for the duration of unavailability. The main question to brainstorm to identify the MTPD is then: can we afford an unavailability this duration, starting from 1 second, continuing to 30 days. This scanning ends at last "yes" answer to this question.

To determine the Asset Value (in Availability), the Security Risk Manager (SRM), in consultation with the System Owner and the Data Owner, will determine the highest possible impact level for the loss of availability (which usually occurs for permanent loss of the asset). This Valuation in terms of Availability is then performed similarly to valuation in terms of Confidentiality and Integrity, by assessing the consequences of a loss of accessibility, assuming a duration of unavailability greater than the MAO to capture the highest possible impact which will materialise after this duration, using the impact scales from Annex B.1.

Duration of Unavailability	Mapping with BC framework
1 second	
10 seconds	
1 minute	
10 minutes	
1 hour	
6 hours	**Critical**
12 hours (1 day)	
24 hours (1 day)	
48 hours (2 days)	
3 days	**Essential**
5 days	
7 days	
15 days	Necessary
30 days	

Table 3-1 – Thresholds for the duration of unavailability

The notion of Business Impact Assessment (BIA) also exists in the Business Continuity framework of the European Commission which focusses on recovery after disasters provoking long periods of unavailability. This framework also uses the notion of Maximum Tolerable Period of Disruption (MTPD), and defines broad bands of unavailability duration to classify systems based on its requirements in term of availability. These broad bands of unavailability, depicted in Table 3-1 – Thresholds for the duration of unavailability, are:

- Critical, for systems having a MTPD up to 48 hours;
- Essential, for systems having a MTPD longer than 48 hours but less than 7 days;
- Necessary, for system having a MTPD between 7 days and 30 days (this third class has been removed from the latest version of the EC Business Continuity framework, but left here for backward compatibility).

If a BC Business Impact Assessment (BIA) has already been performed for the CIS following EC BC Framework, then some business impact has already been estimated for a set of outage durations ('Business Impact Analysis Guidance and Template', section 3.3) which can be reused here. The durations which are also encountered in BC appear in Table 3-1 – Thresholds for the duration of unavailability, in **bold**.

If no BC Business Impact Assessment (BIA) has yet been performed for the CIS, the impact estimates performed as part of this methodology can be reused in a BCP BIA (at least for the durations that also appear in the 'Business Impact Analysis Guidance and Template').

The impact levels for all Security Dimensions are registered for each Primary Asset (as well as the MIPD for the 'Availability' Security Dimension.

Step 3: Identify the impact types included in the description of the worst case scenario

Once Security Risk Manager (SRM) has identified the Security Dimensions (CIA) related with each Primary Asset, s/he will assess the impact types and category (Business or Data Protection) that are most relevant regarding the information provided in the description of the scenario. The Security Risk Manager (SRM) will consult the Impact Scale (Annex B.1 a and b) to determine the types of impact, most relevant to each worst case scenario.

Register the impact types and category identified in each worst case scenario.

Step 4: Select the impact level

To determine the impact level, the Security Risk Manager (SRM) needs to consider which type of effects/consequences are related to the identified impact types. The Impact (Business or Data Protection) Scale (Annex B.1) includes a description of the potential effects of each impact type, mapped with their corresponding level (0 – 10).

Register the effect and level determined for each impact type.

All the information gathered as result of this task will be registered as "Impact scenarios".

Step 5: Consolidate the final impact level from different scenarios

The final result for an asset and Security Dimension is the highest level amongst the different impact scenarios found during brainstorm. As both categories (Business and Data Protection) are taken into account for this maximum, the highest requirement will be considered and not only the business considerations, and protection will be appropriate to the highest concern.

> **NOTE:** This final result for impact will be used with the LIKELIHOOD for the risk calculation in the risk assessment process. The rest of the elements used to build the impact scenario will be registered to keep the traceability of where did the impact value come from.

3.4.3 Primary Asset Attractiveness valuation

The objective of this task is to obtain the values related with the attractiveness of Primary Assets for Potential Adversaries. The attractiveness valuation is obtained through the combination of the POWER and INTEREST of Potential Adversaries that can be motivated by threatening the Primary Asset.

Step 1: Identify Potential Adversaries by interest scenarios

To identify the Potential Adversaries, the Security Risk Manager (SRM) will focus a brainstorming session on the development of scenarios where Potential Adversaries could be interested on the disclosure, modification or unavailability of the identified Primary Assets. The Security Risk Manager (SRM) can use the Catalogue of Potential Adversary types (Annex C.2) to ease the brainstorming.

Step 2: Assessment of POWER of Potential Adversaries

If a Potential Adversary is obtained from the selection provided in the Catalogue of Potential Adversary types (Annex C.2), the POWER value can be obtained from the catalogue. If not, the Security Risk Manager (SRM) will need to determine the POWER.

Step 3: Assessment of the level of INTEREST

The definitions of the INTEREST levels provided in the INTEREST level scale (annex B.2) will provide guidance to the Security Risk Manager (SRM) on the selection of the level of INTEREST of identified Potential Adversaries for the Primary Asset.

Step 4: Selection of the Potential Adversary with the maximum combination of POWER and their INTEREST on the Primary Asset.

The Potential Adversary with the highest value regarding the combination of the Power and INTEREST levels is retained as Attractiveness.

> **NOTE:** The Attractiveness (POWER + INTEREST) of a Primary Asset will be used with the EASINESS of the Threat to assess the LIKELIHOOD of deliberate threats in the Risk Assessment & Evaluation process.

The information related to the interest scenarios will be registered per Primary Asset and per Security Dimension.

3.4.4 Remark on different types of scenarios

In this process, we are assessing the value of Primary Assets by identifying and assessing Impact Scenarios, and their Attractiveness by identifying and assessing Interest Scenarios.

A loss of Confidentiality, Integrity and/or Availability of a Primary Asset is the starting point of these two types of scenario (see Figure 3-2: Difference between the types of scenario):

- an Impact Scenario represents what can happen (bad) after, and due to, the loss of Confidentiality, Integrity and/or Availability of a Primary Asset which could harm – have an impact on – the *organisation*, the *System Owner*, the *Data Owner* or the *Data Subject*; an Impact Scenario starts when there is a loss of Confidentiality, Integrity and/or Availability (due to any possible problem); it ends with an Impact that can be assessed;
- an Interest Scenario represents what can happen (good) after, and thanks to, the loss of Confidentiality, Integrity and/or Availability of a Primary Asset which could be beneficial to a *Potential Adversary*; it is used to estimate the interest of the Potential Adversary which is considered proportional to the benefit it could get out of this loss; an Interest Scenario starts when there is a loss of Confidentiality, Integrity and/or Availability (due to any possible problem); it ends with a possible benefit for the Potential Adversary that can be used to assess its interest to attack the Primary Asset.

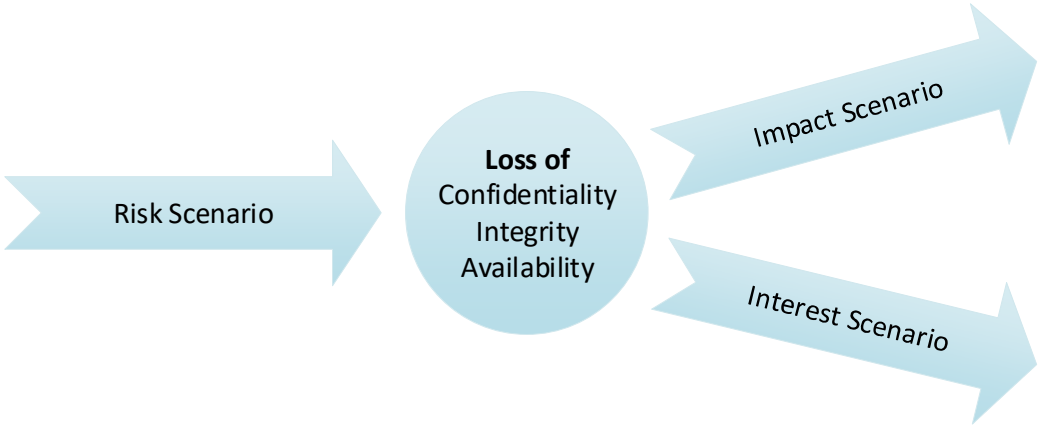


Figure 3-2: Difference between the types of scenario

At a later process (Risk Identification), a third type of scenario, Risk Scenarios, will be introduced to describe what problems could lead to a loss of Confidentiality, Integrity and/or Availability of a Primary Asset:

- a Risk Scenario represents what security event, which threat, can happen on the System which can lead to a loss of Confidentiality, Integrity and/or Availability of a Primary Asset processed therein Figure 3-2: Difference between the types of scenario; such threat can be performed by a *Threat Agent* (intentional threat) or due to an 'Act of God' (unintentional threat); Risk Scenarios are used to identify risks and further assess them; a Risk Scenario ends with a loss of Confidentiality, Integrity and/or Availability;

The term *Threat Agent* is used in defining Risk Scenarios, as the entity which actually perform the Threat. The term *Potential Adversary* is used in defining Impact Scenarios, as the entity that could be interested that the threat occurs. The Potential Adversary can perform the threat him/herself, and act as a Threat Agent, or he/she can be the sponsor of another Threat Agent. In this methodology, we focus on the capacities and interest of the Potential Adversary as he/she can sponsor a Threat Agent.

4 PROCESS 3 – SUPPORTING ASSETS

4.1 Key concepts

- Asset: something worth protecting, either tangible or intangible.
- Supporting Assets**:** Services**,** hardware, software, people, and locations used or involved in the management of the Data and Functions provided by the Target System.
- Service: A service is a means of delivering data processing (Data Sets and Functions) to customers, internally or externally. A Service is made up of a combination of Information Technology products (hardware and software), people and locations. A Service is modelled as a Supporting Asset of type "Service" which is itself made of a sub-set of Supporting Assets.
- Shared service: a Service is shared when its provider makes it available for reuse by other systems. The Risk Study of the Shared Service can be published, entirely or partially, by its Service Provider to be re-used in Risk Studies of CIS that are using the Service.

4.2 Process description

Process ID	RM.P3-SA
Name	P3 – Supporting Assets
Purpose	The objective of this process is to identify and describe the Supporting Assets that make up the Target System and that process Data Sets and perform Functions (Primary Assets).
Outcomes	(1) The Supporting Assets of the Target System are identified and described. (2) Their owners of the Supporting Assets are identified.

4.3 Inputs and Outputs

Inputs	
IN03.01	Catalogue of Supporting Asset type (Annex C.3) Catalogue providing a taxonomy of different types of Supporting Assets, commonly used in the EC environment.
OUT02.01	Primary Asset inventory This inventory includes the identification and description of the Data managed and the Functions provided by the Target System.
Outputs	
OUT03.01	Supporting Asset inventory List of the Target System Supporting Assets, with their corresponding types and owners. Minimum content recommended to build the Supporting Asset inventory: • Supporting Asset ID: An identification of the Supporting Asset. • Supporting Asset Name: The name commonly used in the context of the EC to identify the Supporting Asset (hardware, software, location, etc.). It can be a commercial name (Outlook), or an internal common name (email). • Type: The category to which the Supporting Asset belongs. The Catalogue of Supporting Asset type provides a list of types organised in three levels to facilitate the identification. The level type is selected by the Security Risk Manager (SRM). • Description: A description of the Supporting Asset in relation to the Primary Assets and the rest of relevant Supporting Assets. • Owner: The person, role or entity responsible for the Supporting Asset. Usually, the owner is a member of the information technology department or an external provider.

4.4 Tasks

	SO	DO	LISO	DPC	SRM	IT Staff	HoD
P3 – Supporting Assets							
Supporting Asset Identification	R	-	C	-	R(D)	S	A

4.4.1 Supporting asset identification

The goal of this task is to create an inventory to register the Supporting Assets, to manage the Data and Functions provided by the Target System.

To complete this task, the Security Risk Manager (SRM) may consult the documentation of the Target System, if available. This documentation may include an inventory of hardware and software, a high-level design, an architecture diagram, etc.

Another option to complete the identification of these elements is to obtain them from the System Model developed as a result of the System Modelling process. In any case, the iteration between both tasks (Identification of Supporting Assets and System Modelling) will allow to repeat this task and check that the Supporting Assets included in the inventory are the same to those represented in the system.

At this moment, the Security Risk Manager (SRM) will contact the System Owner to identify which members of the IT department can provide information about the Target System Supporting Assets. This includes system administrators, DataBase Administrators, network managers, Software Architect, service managers, the change management authority, the Project Manager, etc.

5 PROCESS 4 – SYSTEM MODELLING

5.1 Key concepts

- Asset: something worth protecting, either tangible or intangible.
- Primary asset: the Data Sets[8] or Data (for short) managed by the Target System and the Functions[9] provided by it.
- Supporting Assets**:** Services**,** hardware, software, people, and locations used or involved in the management of the Data and Functions provided by the Target System.
- Service: A service is a means of delivering data processing (Data Sets and Functions) to customers, internally or externally. A Service is made up of a combination of Information Technology products (hardware and software), people and locations. A Service is modelled as a Supporting Asset of type "Service" which is itself made of a sub-set of Supporting Assets.
- Shared service: a Service is shared when its Risk Study is published, entirely or partially, by its Service Provider to be re-used in Risk Studies of CIS that are using the Service.
- System Model**:** Representation of the architecture of the system, including primary and Supporting Assets and their relationships. The System Model will be used in the risk assessment process to identify relevant applicable threats in the risk identification task and to select applicable Security Measures for the mitigation of risks during the risk treatment process.

5.2 Process description

Process ID	RM.P4-MOD
Name	P4 – System Modelling
Purpose	The objective of this process is to build a model of the Target System in terms of Primary and Supporting Assets and their relationships.
Outcomes	(1) A model of the Target System in terms of Primary and Supporting Assets and their relationships. (2) For each Supporting Asset, a list of Primary Assets it processes (Data Sets) and perform (Functions), with their value.

5.3 Inputs and Outputs

Inputs	
OUT02.01	Primary asset inventory List of Primary Assets obtained from the Primary Asset Analysis process.
OUT03.01	Supporting asset inventory List of the Target System Supporting Assets, with their corresponding types and owners.
Outputs	
OUT04.01	System Model Conceptual model resulting from system modelling task, representing the primary and Supporting Assets related to the Target System.

[8] Commission Decision 46/2017: A Data Set is a set of information which serves a specific business process or activity of the Commission.

[9] Commission Decision 46/2017: 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.

5.4 Tasks

	SO	DO	LISO	DPC	SRM	IT Staff	HoD
P4 – System Modelling							
System Modelling	R	I	C	-	R(D)	S	A

The IT staff will be consulted to verify and complete the System Model.

5.4.1 System Modelling

The objective of this task is to develop a System Model to ease performing further Risk Management processes, notably:

- Risk Identification: Threat Analysis is facilitated if the brainstorming can be done on a drawing / model of the target System;
- Risk Treatment: the selection of Security Measures, especially the Supporting Asset where they should be applied, is easier with the help of a drawing / model.

The ITSRM Methodology proposes currently three models described below. Their aim is to represent, in a useful manner, the Primary Assets identified in P2, the Supporting Assets identified in P3, and their relationships.

Other models could be useful, such as a logical model, enterprise architecture model, and business process model. However the bare minimum is to record, for each Primary Asset, all the Supporting Assets where it is processed. This is very important as this is where a threat can materialise.

5.4.1.1 Location Matrix Model

This matrix is built by putting all identified Primary Assets in one dimension, by putting all identified Supporting Assets on the other dimension, and by flagging the intersection when the Primary Asset can be found on the Supporting Asset.

	Primary assets		
Supporting asset	PA1	PA2	PA3
SA1	X		X
SA2		X	

To obtain the information required to complete this task, the Security Risk Manager (SRM) will develop a brainstorming session and obtain information about the Hardware, Software, services, locations and people that manage the Target System Primary Assets.

5.4.1.2 Service Modelling

A Service is a special Supporting Asset of type “service”. It is defined recursively as a Supporting Asset made of other Supporting Assets (i.e. hardware, software, people, location and … Service). More simply, a Service is a Supporting Asset, of type “service”, used to regroup other Supporting Assets. A Service can also be seen as a sub-part of a CIS processing functions and data sets in service mode.

Consequently, in practice, a Service is defined by:

- a Supporting Asset of type “service”;
- a sub-set of Supporting Assets that build the Service;
- a sub-set of Primary Asset Containers, located on the sub-set of Supporting Assets, representing Functions and Data Sets processed by the service.

A Service with its Primary Asset Containers is the key concept to model the re-use in a CIS of a Service, provided by a Service Provider in another CIS.

To illustrate this, we will model a simplified CIS supporting a generic client/server application. If drawn by one System Owner mastering the whole system, the model could look like in the Figure 5-1: Model of a simple system entirely known by System Owner:

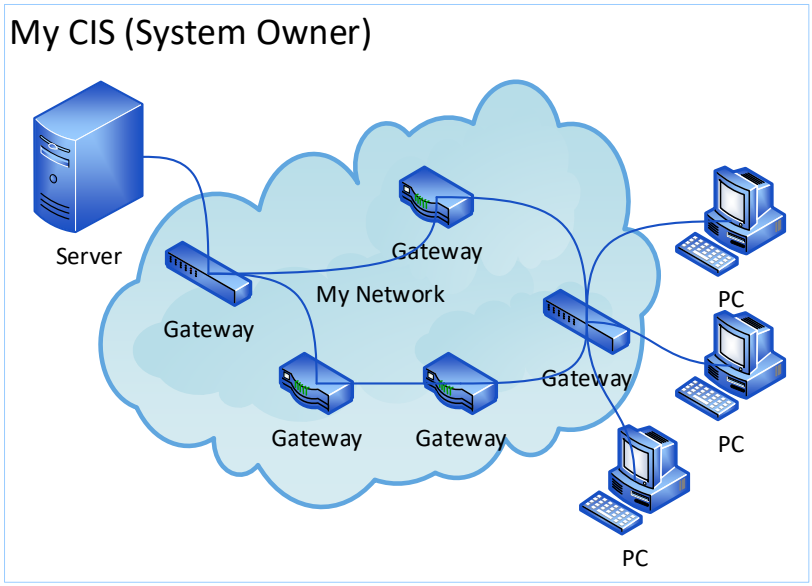


Figure 5-1: Model of a simple system entirely known by System Owner

This model includes all supporting assets of the system and regroups internally the network gateways and media links into the Network Service "My Network".

If the System Owner prefers to reuse a Network Service which is provided by a Service Provider, the single model can be split into two models like in the Figure 5-2: Same system modelled in two parts by System Owner and Service Provider:

1. the model of the CIS which can be simplified by its System Owner; the Network Service "My Network" is model as a Network Service without knowing anything about the Supporting Assets it is made of; the System Owner can then choose to reuse an externally provided service for its Network service;
2. the model of the "Provided Network" is detailed by its Service Provider (the System Owner of the provided service); the Service Provider can then share its Service so that other System Owners can use it.

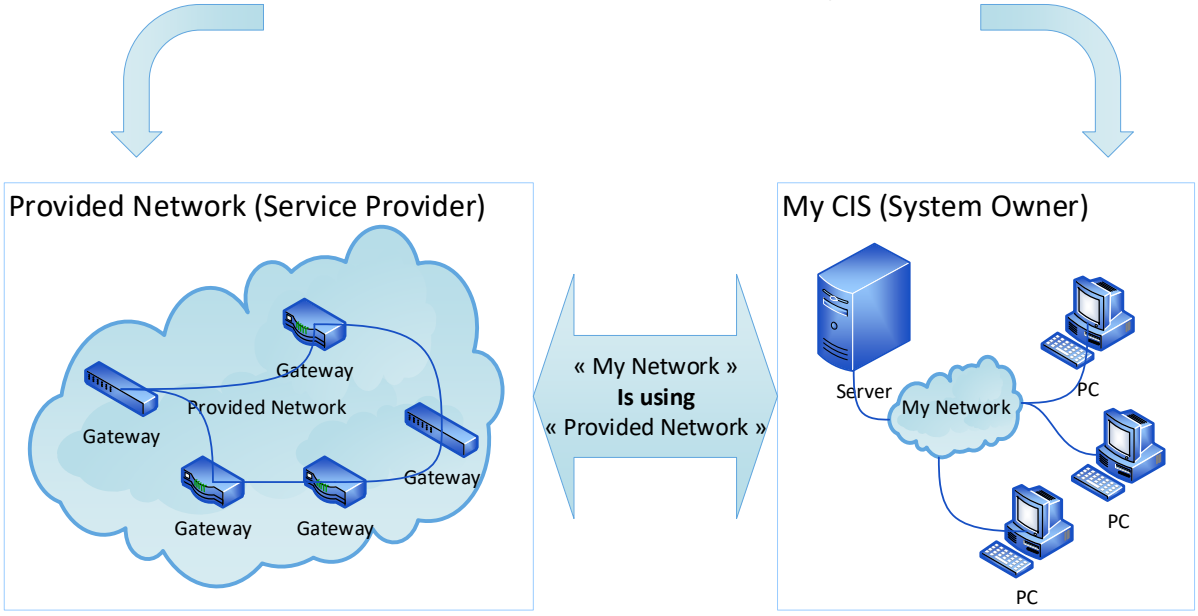


Figure 5-2: Same system modelled in two parts by System Owner and Service Provider

The Risk Assessment and Treatment can be accordingly split into two studies, one done by the CIS System Owner, the other by the Service Provider. In addition, considering the provided Service is shared and re-used from an

architectural point of view, risks can be shared accordingly from a Risk Management point of view. This will simplify Risk Studies for CIS re-using external components (Services) whose Risk Study has already been done and shared. Primary Asset Containers define the interface between the Service provider and the Service user:

- the Service Provider should define at least one Primary Asset Container for the Service provided to represent the Primary Asset that is processed in the service; as described in P2, the exact characteristics of Primary Assets are not known at Service design, so they are usually set by assumption, which is exactly the purpose of Containers;
- the Service user can then "put" its actual Primary Assets in the Primary Asset Containers of the re-used Service, "putting" the actual characteristics – known at Service client's side – in the Containers.

An analogy with the world of programing languages might help in understanding this concept. A Service is like a function, which is defined by a list of arguments that are used in the code of the function. The containers are like the parameters of the service / function. When a developer wants to call the function, the actual values are passed as arguments to the function. Similarly, when a CIS wants to re-use a shared service, the actual Primary Asset is passed through it via the Containers.

5.4.1.3 System Architecture Model

Brainstorming can be facilitated with a drawing of the system, representing the "flow" of Primary Assets on a "geographical" picture of the Supporting Assets.

Different models may be used and combined, such as:

- Data Flow Diagram;
- Network/System Architecture;
- Software Architecture.

For this, the Security Risk Manager (SRM) can reuse models that are developed during software development for example.

The Security Risk Manager (SRM) will draw the elements identified as Supporting Assets from the description provided by the System Owner during the brainstorming session.

It is also required to draw the relations between Supporting Assets to complete the System Model. For example, networks and cables connecting hardware's, users in front of their equipment, network stack on their processing hardware, hardware in rooms and buildings.

5.4.1.4 Use of models

At this stage, these models might already be used for cross-checking the completeness of the inventory of Primary and Supporting Assets: the Security Risk Manager (SRM) can validate the selection of Primary and Supporting Assets, and complete and/or validate the System Model.

As part of the iteration of this process, the Security Risk Manager (SRM) will then go back to the Supporting Asset inventory and complete any missing information regarding the identification of additional Supporting Assets related to the Target System Data and Functions.

All Primary Assets should be mapped to at least one Supporting Asset. If there is any Data or Function not linked to a Supporting Asset, the Security Risk Manager (SRM) should review the System Model with the System Owner to identify what HW, SW, people….is missing.

> IMPORTANT: **The level of detail in the System Model will determine the scope of the risk assessment and the granularity of the selection of applicable Threats and Security Measures.** The more detailed is the model, the more detailed the results of the Risk Assessment and Treatment will be. When the SRM iterates on modelling to enrich the model, (s)he will also go into further detail in the result of the Risk Management. If the SRM excludes part of the system in its model, the Risk Study will not give results on this part. If the SRM makes assumptions in the model, the Risk Study will be based on these assumptions. **The concept of model is key in ITSRM Methodology: grouped with the built-in iterative capacity of the methodology, it allow the Security Risk Manager (SRM) to produce quickly a high-level Risk Study, and then refine it continuously as more details or more alternatives are known.**

6 PROCESS 5 – RISK IDENTIFICATION

6.1 Key concepts

- Risk scenario: Combination of:
  (1) a Primary Asset,
  (2) a Security Dimension,
  (3) a Threat that can harm this Security Dimension for this Primary Asset, and
  (4) the Supporting Asset on which the Primary Asset is located and where the Threat materialises.
- Threat analysis: identification of relevant threats for each combination of 1) a Primary Asset, 2) a Security Dimension and 3) a Supporting Asset. This identification is based on the System Model.
- Risk Owner: The risk owner is defined in ISO/IEC 27001:2013 as the person or entity with the accountability and authority to manage a risk. The System Owner is responsible for the security risk management process for an information system and for the continual monitoring of risks and regular reviews of the risk management decisions. Following [CD46/2017], the Head of Department is the Risk Owner of all risks identified in its Target Systems.
- Target of a Security Measure: the target of a Security Measure is the place where the measure can be actually implemented. Such target can be the organisation (e.g. a general security policy), the system (e.g. Risk Management, Code review, vulnerability scan) or a particular Supporting Asset (e.g. encryption on a data link or a hard disk, access control to an Operating System).

6.2 Process Description

Process ID	RM.P5-RID
Name	P5 – Risk Identification
Purpose	The objective of the risk identification is to identify risks that will be analysed, evaluated and treated in next processes.
Outcomes	(1) A list of risks identified as a risk scenario. (2) Existing Security Measures (in the case of an already existing target system) are identified.

6.3 Inputs and Outputs

Inputs	
OUT04.01	System Model Conceptual model resulting from the system modelling task that represents the primary and Supporting Assets related to the Target System.
IN05.01	Threat catalogue Selection of threats mapped with the type of SA and Security Dimension (CIA) they might affect.
OUT01.05	Security Measures Register
Outputs	
OUT05.01	Risk Scenarios The list of risk scenarios envisaged during the threat analysis. Minimum content recommended to build the Risk Scenarios: • Risk ID: an identification of the Risk. • Primary Asset ID: an identification of the Primary Asset. • Security Dimension threaten: Confidentiality, Integrity or Availability. • Supporting Asset ID: an identification of the Supporting Asset. • Threat ID: an identification of the Threat.
OUT01.05	Security Measures Register: The list of Security Measures selected for the Risk Management. Minimum content recommended:

	• Security Measure ID: Identification of the Security Measure. • Target of the measure**:** Either 'Organisation', 'System', or the Supporting Asset ID (identification of the Supporting Asset on which the measure will be applied/implemented to reduce the risk). • A flag (I): specifying that the Security Measure is an existing one (already implemented before Risk Treatment).

6.4 Tasks

	SO	DO	LISO	DPC	SRM	IT Staff	HoD
P5 – Risk Identification							
Risk Identification	R	I	C	I	R(D)	C	A
Existing Security Measures Identification	R	I	S	I	R(D)	S	A

6.4.1 Risk Identification

The objective of the risk identification task is to build the risk scenarios that will be analysed in this process. The risk scenarios are used to represent the risks for the organisation regarding the consequences of potential threats in relation to the confidentiality, integrity and availability of the Primary Assets.

The System Model will support the selection of relevant threats required for the execution of the risk identification task. The Security Risk Manager (SRM) will consult the System Model to identify on which Supporting Asset the Primary Assets could be threatened.

To identify the specific elements related to each risk scenario, the Security Risk Manager (SRM) will work with relevant IT staff with knowledge on the technical characteristics of the identified Supporting Assets. This approach is determined to ensure that the threats are identified considering the technical characteristics of the Supporting Assets.

Method: The recommended approach to complete this task is to develop a Threat Modelling, using the System Model (in P4 – System Modelling) and the selection of threats provided in the Catalogue of Threats (Annex C.4). This is also referred to as Threat Analysis, or Architecture Risk Analysis (ARA).
To perform the threat analysis, the Security Risk Manager (SRM) will follow:

- Step 1: Consult the System Model to identify the combination of Primary Asset/Security Dimension/Supporting Assets to be considered in the threat analysis. The System Model provides a useful instrument to identify most pertinent threats regarding the architecture of the system. If a specific combination of Primary Asset and Security Dimension is managed by different types of Supporting Assets, all of them should be registered and considered independently as different risk scenarios.
- Step 2: To complete the threat analysis the Security Risk Manager (SRM) needs to consider which potential threats are most likely to affect the confidentiality, integrity or availability of the Primary Assets regarding the type of Supporting Assets that were used. The use of the information provided in the threat catalogue will allow filtering the selection of applicable threats regarding the Security Dimension and Supporting Asset type identified in each risk scenario.

To perform Threat Modelling, the Security Risk Manager (SRM) should look at the model of the System as an attacker would look at the system, finding ways to attack it, to provoke loss of Confidentiality, Integrity and/or Availability of Primary Assets where they can be found on the system.

6.4.2 Existing Security Measures identification

When the Target System already exists, the Security Risk Manager (SRM) should identify Security Measures which are already implemented, to avoid the duplication of Security Measures in next processes.

The following sources of information might be useful in identifying existing Security Measures:

- existing risk treatment plans;

- on-site review;
- results of audits or checks already performed.

The identification of existing security measures is usually completed during the execution of the Risk Identification process because, in practice, such measures are often popping up during discussions aiming at identifying risks. However, existence of such measures can be signalled at any step of the Risk Management and should be recorded as soon as the Security Risk Manager (SRM) is made aware of it.

The concepts of Target and Sophistication Level of a Security Measure will be defined and used in P6 and P7. Basically, the Target of a Measure is the detailed place where it is implemented; and its Sophistication Level is an assessment of the level of complexity of its implementation, proportionate to its "strength" as counter measure. The Security Risk Manager (SRM) can already record these two parameters if known at this stage.

6.4.3 Specific case: risk identification when shared services are re-used

As described in the modelling process, the model of the system will determine the Risk Study, particularly the Risk Identification. This can be exemplified in the specific context of modelling the re-use of a service by a system. In this case, the Risk Identification can be performed iteratively as described below.

6.4.3.1 Modelling a service without any further detail

In a first iteration, the Security Risk Manager (SRM) can just create a Supporting Asset of type "service".

With this initial model, risks based on threats applicable to a Service, to any kind of service, can already be identified. This is the case, for example, for risk of loss of governance that can occur in any outsourced service.

6.4.3.2 Modelling a service with assumptions on its generic building blocks

In an iteration, the Security Risk Manager (SRM) could made assumptions on the service and how it is probably made of. For example, one can assume that the service will use a generic server and its Operating System. The model could be consequently enriched by adding two Supporting Assets to the Service: 1) Hardware – Server, and 2) Software – Middleware – Operating System.

With these assumptions, the model is enriched and risks applicable to Hardware and Software could be identified and added to the Risk Study. These risks are somehow generic but can be used in further Service Level Agreements to be established with a service provider.

This is not a mandatory iteration but this shows that the model determines the risk study in terms of results, also in the foreseen use of these results. Such high-level risk assessment and treatment based on putting hypothesis on the system can provide reasoning, rational and documentation to define statements in a Service Level Agreement with a potential provider.

6.4.3.3 Modelling a service re-using an existing service provided externally

If it is decided, or assumed, that a known externally provided service will be re-used, the Security Risk Manager (SRM) can declare this use by linking the Service in the current model with the service externally provided.

Then, if a Risk Study is available for the externally provided service, pertinent risks identified in the external service can be merged in the current Risk Register. Later on, these imported risks can be considered as shared risks (see Risk Treatment).

7 PROCESS 6 – RISK ANALYSIS AND EVALUATION

7.1 Key concepts

- EASINESS: Valuation of the effort required to materialise a given intentional threat. This value is inversely proportional to the effort required to perpetrate the threat in terms of time, money, technical knowledge, capabilities and skills.
- FREQUENCY: Description of the values (expressed qualitatively and quantitatively for risk calculation) used to express the periodicity of accidental threats from materialising *(ITSRM² v1.0)*.
- POWER: Potential Adversaries can be characterised by their POWER (their available capacity to perform a threat) and their Interest (their willingness to use their capacity to threaten a given asset).
- Attractiveness: The maximum combination of POWER and INTEREST for a Potential Adversary, for a given Primary Asset and Security Dimension.
- LIKELIHOOD: Measured for accidental threats as the FREQUENCY of occurrence and for deliberate threats as the combination of the POWER and INTEREST of Potential Adversaries with the threat EASINESS *(ITSRM² v1.0)*.
- Inherent Risk: The Risk without taking any Security Measure into account *(ITSRM² v1.0*. In some circumstances, it might be difficult to imagine a situation without any security measure. So, the notion of Inherent Risk can sometimes be seen as theoretical. But in the ITSRM Methodology, this notion is used in practice to assess the residual risk by applying cumulated reduction to the Inherent Risk, corresponding to cumulated measures.
- Residual risk: The Risk which remains after mitigation by Security Measures *(ITSRM² v1.0)*.
- Sophistication Level: each Security Measure can be implemented in different ways, reducing a risk to a smaller or larger degree. In this methodology, it is assumed that possible implementations of a measure can be grouped, defined and ordered into three "strength" levels. These are defined as Sophistication Levels. For example, implementing the Authentication Measure with Single Factor Authentication or Two-Factor Authentication might lead to two different Sophistication Levels.
- Mitigation Factor: The Mitigation Factor measures the effectiveness of a Security Measure to mitigate the CONSEQUENCE and/or the LIKELIHOOD of a risk caused by a specific threat. It is a percentage which estimate the "strength" of reduction of a Security Measure on the CONSEQUENCE and/or the LIKELIHOOD of a given Threat. Two Mitigation Factors can be assessed for a Security Measure: one mitigating the CONSEQUENCE, one mitigating the LIKELIHOOD. In addition, as the Security Measure can be implemented in 3 different Sophistication Levels, each Security Measure can have 6 Mitigation Factors, which can be noted:

	Threat (T_j)			
Security Measure (SM_i)		Sophistication Level (SL)		
	Parameter	1	2	3
	LIKELIHOOD	MF1L	MF2L	MF3L
	CONSEQUENCE	MF1C	MF2C	MF3C

7.2 Process description

Process ID	RM.P6-RAE
Name	P6 – Risk Analysis and Evaluation
Purpose	The objective of the risk analysis and evaluation process is the computation of the RISK LEVEL for each risk identified in the previous process. When no Security Measure has been identified to modify the risk (typically at first iteration of P6), this is the Inherent RISK LEVEL. As soon as Security Measures have been identified to modify the risk, as part of further risk treatment (P7) iteration, it becomes a Residual RISK LEVEL based on the list of Security Measures identified. The list of Risks is sorted by Residual RISK LEVEL to ease risk evaluation.

Outcomes	(1) A sorted list of risks with Residual RISK LEVEL.

7.3 Inputs and Outputs

Inputs	
OUT02.01	Primary asset inventory List of Primary Assets obtained from the Primary Asset Analysis process. From this list, the Security Risk Manager (SRM) will use the asset value and its attractiveness.
OUT05.01	Risk scenarios
IN05.01	Catalogue of Threats (Annex C.4)
IN06.01	Catalogue of Security Measures (Annex C.5)
IN06.02	Risk Scale (Annex B.3)
OUT07.01	Treatment Register
OUT01.05	Security Measures Register
Outputs	
OUT06.01	Risk register The information included in this output will collect the Inherent RISK LEVEL and the Residual RISK LEVEL. This information will guide the risk treatment decisions required as result of the execution of the tasks foreseen in the next process. This contains: • Risk ID: identification number for the risk. • CONSEQUENCE: from the Primary Asset inventory • LIKELIHOOD: from the Primary Asset inventory and the Risk Scenarios • Inherent RISK LEVEL: RISK LEVEL obtained before the application of the mitigation values of implemented Security Measures (calculated from CONSEQUENCE and LIKELIHOOD). • Reduced CONSEQUENCE: after application of Mitigation Factors from the Treatment Register • Reduced LIKELIHOOD: after application of Mitigation Factors from the Treatment Register • Residual RISK LEVEL: RISK LEVEL obtained after the application of the mitigation values of implemented Security Measures (calculated from Reduced CONSEQUENCE and Reduced LIKELIHOOD).

7.4 Tasks

	SO	DO	LISO	DPC	SRM	IT Staff	HoD
P6 – Risk Analysis & Evaluation							
Risk Analysis	R	-	-	-	R(D)	-	A
Risk Evaluation	R	I	C	C	R(D)	I	A

7.4.1 Risk Analysis

The objective of the risk analysis task is to calculate the RISK LEVEL and/or the Residual RISK LEVEL of Risks identified.

7.4.1.1 Inherent RISK LEVEL

The CONSEQUENCE is the Primary Asset Value as assessed in P2.

The LIKELIHOOD is related to the type of threats and the Potential Adversaries, identified for the combination of PA, Security Dimension and SA included in each risk scenario.

- If the type of threat included in a risk scenario is accidental, the LIKELIHOOD will correspond to the threat FREQUENCY. The FREQUENCY is a value between 1-5, used to express the periodicity of accidental threats from materialising, considering past experience or relevant published information. A value for FREQUENCY will be proposed for each accidental threat in the Extended Catalogue of Threats (see remarks in Annex C.4). These values provided are mapped with the levels and definitions included in the threat FREQUENCY scale (annex B.3).
- If the type of threat included in the risk scenario is deliberate, the LIKELIHOOD will correspond to the average of the threat EASINESS, the Potential Adversary POWER and its INTEREST (as retained in the Attractiveness).
    - A value for EASINESS will be proposed for each deliberate threat in the Extended Catalogue of Threats (see remarks in Annex C.4). This value assesses the technical difficulty associated to each threat and can be assessed based on the scale provided in Annex B.3.
    - The POWER of Potential Adversaries is assessed in the Primary Asset process.
    - The INTEREST of Potential Adversaries is assessed in the Primary Asset process.
- In cases where a threat can be caused accidentally or deliberately, the Security Risk Manager (SRM) should keep the option that gives the highest resulting LIKELIHOOD.
- If the threat included in a risk scenario is not obtained from the selection provided in the Catalogue of Threats (Annex C.4), the Security Risk Manager (SRM) should identify the threat type (accidental or deliberate) and determine the values needed for the estimation of the LIKELIHOOD (EASINESS for deliberate threats and FREQUENCY for accidental threats).

Note: Values for FREQUENCY and/or EASINESS are propositions in the extended Catalogue of Threats: the Security Risk Manager (SRM) is free to propose different values as long as this modification is clearly flagged and justified, recorded as an exception in the current Risk Study.

Remark: To keep the coherence and homogeneity of results, the Security Risk Manager (SRM) should apply the same range of values as those provided in the threat catalogue to determine the threat FREQUENCY (see Annex B.3 for the definition of the values provided for the threat FREQUENCY) and the threat EASINESS. If not, results will not be comparable with other risks obtained from the application of this methodology.

The RISK LEVEL or Inherent RISK LEVEL (level of risk before treatment i.e. with no Security Measures taken into account) is the product of the LIKELIHOOD and the CONSEQUENCE assessed above. It can be represented on the following Risk Matrix (also known as Risk Heat Map), by using the LIKELIHOOD and the CONSEQUENCE assessed above as coordinates.

CONSEQUENCE						
	10	10	20	30	40	50
	9	9	18	27	36	45
	8	8	16	24	32	40
	7	7	14	21	28	35
	6	6	12	18	24	30
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		LIKELIHOOD				

7.4.1.2 Residual RISK LEVEL

The Residual RISK LEVEL (risk after implementation of a set of Security Measures to mitigate it) is also calculated as the product of a LIKELIHOOD and a CONSEQUENCE. And it can also be mapped the same way on the Risk Matrix by using these LIKELIHOOD and CONSEQUENCE as coordinates.

But for the Residual RISK LEVEL, the product is based on a LIKELIHOOD and a CONSEQUENCE reduced due to the chosen mitigating measures.

The reduction of LIKELIHOOD and of CONSEQUENCE are calculated based on the two Mitigation Factors of the Security Measures chosen to mitigate the Threat identifying the given risk:

$$\text{Reduced CONSEQUENCE} = \text{CONSEQUENCE} * (1 - MFC[SM_1,SL]) * \ldots * (1 - MFC[SM_n,SL])$$

$$\text{Reduced LIKELIHOOD} = \text{LIKELIHOOD} * (1 - MFL[SM_1,SL]) * \ldots * (1 - MFL[SM_n,SL])$$

Where:

- SMi (i=1..n) are the n Security Measures chosen to mitigate the Risk;
- SL is the Sophistication Level chosen for the Security Measure.

The Residual RISK LEVEL (level of risk after treatment) is the product of the Reduced LIKELIHOOD and the Reduced CONSEQUENCE assessed above, after cumulative application of the Mitigation Factors of the chosen Security Measures.

A Cumulated Mitigation Factor for a subset of Security Measures can be defined as the following product based on Mitigation Factors of the n Security Measures building the subset:

$$\text{Cumulated Mitigation Factor} = (1 - MFx\ [SM_1,SL]) * \ldots * (1 - MFx\ [SM_n,SL])$$

This Residual Risk can be represented on the Risk Matrix by using the Reduced LIKELIHOOD and the Reduced CONSEQUENCE assessed above as coordinates.

7.4.2 Risk Evaluation

The objective of the risk evaluation task is to order risks and ease the selection of the Risks that require a further treatment because considered as unacceptable as such.

Risks may be ordered from the highest to the lowest Residual RISK LEVEL and/or Reduced CONSEQUENCE and/or Reduced LIKELIHOOD.

The information related to the risk scenarios and the implemented Security Measures will be recorded in the Risk Register (OUT06.01). This register will be used as input of the Risk Treatment process to include the risk treatment options and allow the implementation of additional Security Measures to reduce risk to acceptable levels.

7.4.3 Specific case: risk analysis when shared services are re-used

As described in the modelling process, the model of the system will determine the Risk Study. This was exemplified in the Risk Identification by showing how risks identified in a Risk Study of an externally provided service can be merged in the risk register of the system re-using the service.

Those risks were already analysed in the context of the shared service. This means that Inherent RISK LEVELS have been calculated with the different parameters from the Risk Analysis of the shared service: values of Primary Assets, POWER and INTEREST of their Potential Adversaries, and Frequency/Easiness of threats. And Residual RISK LEVELS have been calculated with the different parameters from the Risk Treatment of the Shared Service: Sophistication Level and Mitigation Factors of the Security Measures selected.

When re-using a Shared Service, it can be assumed that only parameters related to Primary Assets will change: threats stay the same and the same risk treatments are applied. Consequently, RISK LEVELS can be recomputed in the context of the using system by simply replacing the parameters related to Primary Assets in the formulas i.e. by taking values, POWER and INTEREST of the Primary Assets in the context of the using system.

8 PROCESS 7 – RISK TREATMENT

8.1 Key concepts

- Asset: something worth protecting, either tangible or intangible.
- Supporting Assets**:** Services**,** hardware, software, people, and locations used or involved in the management of the Data and Functions provided by the Target System.
- Risk Treatment options: there are 4 options to treat a risk:
  - *Risk Modification: introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable (ISO 27005:2018); risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation" […] and "risk reduction"*
  - *Risk Retention: decision on retaining the risk without further action taken depending on risk evaluation* (ISO 27005:2018);
  - Risk Avoidance: *the activity or condition that gives rise to the particular risk should be avoided* (ISO/IEC 27005:2018);
  - Risk Sharing: *the risk should be shared with another party that can most effectively manage the particular risk depending on risk evaluation* (ISO 27005:2018).
- Sophistication Level: each Security Measure can be implemented in different ways, reducing a risk to a smaller or larger degree. In this methodology, it is assumed that possible implementations of a measure can be grouped, defined, and ordered into three "strength" levels"". These are defined as Sophistication Levels. For example, implementing the Authentication Measure with Single Factor Authentication or Two-Factor Authentication might lead to two different Sophistication Levels.
- Target of a Security Measure: the target of a Security Measure is the place where the measure can be actually implemented. Such target can be the organisation (e.g. a general security policy), the system (e.g. Risk Management, Code review, vulnerability scan) or a particular Supporting Asset (e.g. encryption on a data link or a hard disk, access control to an Operating System).
- Mitigation Factor: The Mitigation Factor measures the effectiveness of a Security Measure to mitigation the CONSEQUENCE and/or the LIKELIHOOD of a risk caused by a specific threat. It is a percentage which assesse the "strength" of reduction of a Security Measure on the CONSEQUENCE and/or the LIKELIHOOD of a given Threat. Two Mitigation Factors can be assessed for a Security Measure: one mitigating the CONSEQUENCE, one mitigating the LIKELIHOOD. In addition, as the Security Measure can be implemented in 3 different Sophistication Levels, each Security Measure can have 6 Mitigation Factors which can be noted:

	Threat (T_j)			
Security Measure (SM_i)		Sophistication Level (SL)		
	Parameter	**1**	**2**	**3**
	LIKELIHOOD	MF1L	MF2L	MF3L
	CONSEQUENCE	MF1C	MF2C	MF3C

8.2 Process description

Process ID	RM.P7-RT
Name	P7 – Risk Treatment
Purpose	The objective of the risk treatment process is the selection of the risk treatment options that are most appropriate in relation with the identified risks and the constraints of the organisation. Focus is on the modification option which requires selecting mitigating Security Measures to reduce the risks.
Outcomes	(1) A risk treatment register that gathers all the information related to the risk treatment options and applicable Security Measures in case of mitigation.

8.3 Inputs and Outputs

Inputs	
OUT03.02	System Model
OUT05.01	Risk scenarios
OUT06.01	Risk register
OUT07.01	Treatment Register As Risk Treatment will be repeated a lot of times, the Treatment Register is considered an output as well as an input to the process. Its detailed description can consequently be found in the outputs section just below.
OUT01.05	Security Measures Register
IN06.01	Catalogue of Security Measures (Annex C.5)
Outputs	
OUT07.01	Treatment Register List of the treatments linked to the treated risk, with details corresponding to the treatment option (notably a link to the Security Measure chosen for modification option). Minimum content recommended: • Treatment ID: identification of the treatment • Risk ID: identification of the risk treated (from Risk Scenarios) • Type of treatment: Modification, Retention, Avoidance, Sharing. • Motivation: optional description of the reason to choose this treatment When the treatment option chosen is "Modification of Risk", the following parameter must be added: • Security Measure ID: link to the Security Measure (SM_i) chosen to reduce the risk (from the Security Measures Register).
OUT01.05	Security Measures Register: The list of Security Measures selected for the Risk Management. Minimum content recommended: • Security Measure ID: Identification of the Security Measure. • A flag (R): specifying that the Security Measure is selected to reduce a Risk. • Security Measure Sophistication Level: the sophistication level chosen for the Security Measure (x). • Security Measure Mitigation Factors: assessment of the Mitigation Factors for the chosen Sophistication Level, both for CONSEQUENCE and LIKELIHOOD (MFxC and MFxL). • Target of the measure**:** Either 'Organisation', 'System', or the Supporting Asset ID (identification of the Supporting Asset on which the measure will be applied/implemented to reduce the risk).

8.4 Tasks

	SO	DO	LISO	DPC	SRM	IT Staff	HoD
P7 – Risk Treatment							
Selection of Risk Treatment Options	R	I	C	C	R(D)	-	A
Detailing the Treatment	R	I	C	C	R(D)	C	A

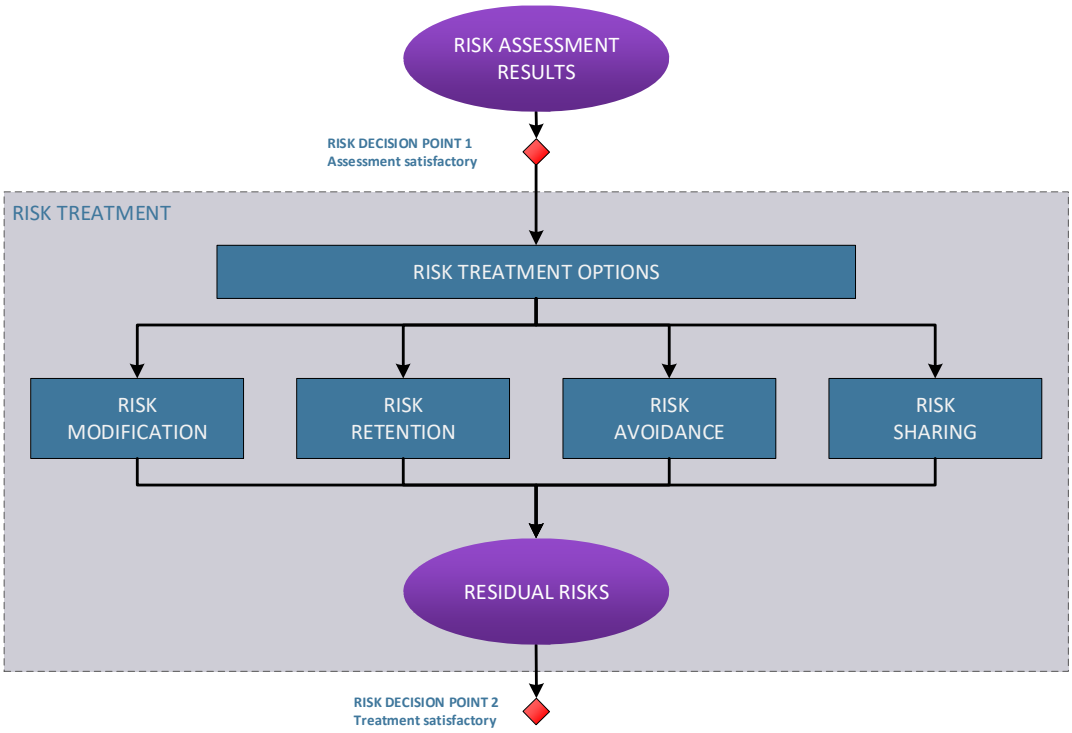
8.4.1 Selection of risk treatment options

Through this task the Security Risk Manager (SRM) will determine the best risk treatment option(s) to propose to the System Owner for each risk scenario included in the risk register resulting from P6.

The selection of the risk treatment options can be complemented with a description of the motivations for their selection.

This selection will mainly be based on *the expected cost for implementing these options*, on constraints or requirements determined during System Security Characterisation, *and on the expected benefits from these options*.

The four possible options are not mutually exclusive Figure 8-1: Risk treatment activity (ISO 27005). The Security Risk Manager (SRM) can select a combination of treatments of different types for a given risk. Usually, a Security Risk Manager (SRM) will select several times Risk Reduction option (i.e. several Security Measures) and/or Risk Sharing option, and finally will propose to accept the Residual Risk (retaining risk after these treatments). Often, risk avoidance will be chosen if the risk is too high or if the cost of mitigating it would exceed the benefit in terms of reduction.



(source: ISO/IEC 27005:2018 - Figure 3 – The risk treatment activity)

Figure 8-1: Risk treatment activity (ISO 27005)

After a modification of the risk treatment options, the Security Risk Manager (SRM) will loop back to the Risk Analysis and Evaluation process to calculate Residual RISK LEVELS if the proposed risk treatment options were in place. As the acceptance of the outcomes of the Risk Management exercise implies the formal acceptance of all Residual Risks, the Analysis-Evaluation-Treatment loop can stop when the System Owner could be comfortable accepting the Residual Risks.

In practice, it can also happen that the Risk Management exercise is time-boxed. Prioritising the risks with the highest Residual RISK LEVEL ensures the smallest possible value for the maximum Residual RISK LEVELS, among all prioritisation strategies.

8.4.2 Detailing the treatment

The schema proposed in the Figure 8-1: Risk treatment activity (ISO 27005) from ISO/IEC 27005:2018 is rather theoretical and static. We propose hereafter a more pragmatic approach to risk treatment summarised in the Figure 8-2: Pragmatic Risk Treatment:

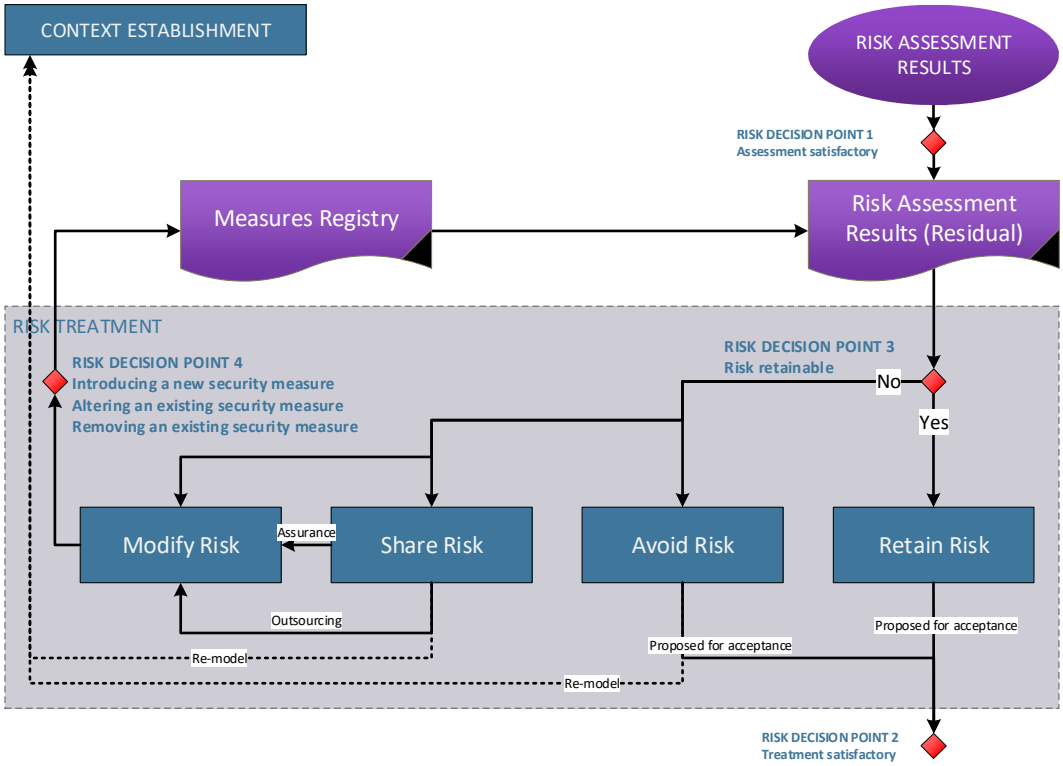


Figure 8-2: Pragmatic Risk Treatment

The process of the different risk treatment options provided in this methodology are detailed in the following sections.

8.4.2.1 Risk retention

This option will be identified, possibly after other risk treatments, for risks having a (Residual) RISK LEVEL considered as acceptable by the SRM. These risks can consequently be proposed for formal acceptance.

If the level of (residual) *risk meets the risk acceptance criteria, there is no need for implementing additional controls and the risk can be retained.*

In theory, *risk acceptance criteria should be developed and specified* before risk assessment and treatment. As risk acceptance criteria often *depend on the organisation's policies, goals, objectives and the interests of stakeholders*, they could be specified at the level of the organisation.

Nevertheless, in practice, *risk acceptance can be more complex than just determining whether or not a residual risk falls above or below a single threshold.* Moreover, it can even be impossible to have a generic criteria at the level of the organisation, fitting all its Departments, businesses and systems.

In addition, *in some cases the level of residual risk may not meet risk acceptance criteria because the criteria being applied do not take into account prevailing circumstances. For example, it might be argued that it is necessary to accept risks because the benefits accompanying the risks are very attractive, or because the cost of risk modification is too high. Such circumstances indicate that risk acceptance criteria are inadequate and should be revised if possible.*

However, it is not always possible to revise the risk acceptance criteria in a timely manner. In such cases, decision makers may have to accept risks that do not meet normal acceptance criteria. If this is necessary, the decision maker should explicitly comment on the risks and include a justification for the decision to override normal risk acceptance criteria.

The pragmatic approach proposed to determine risk treatment options has three actions:

- The Security Risk Manager (SRM) can propose a simple Risk Acceptance Criteria based on a threshold on the Residual RISK LEVEL, the Reduced CONSEQUENCE, the Reduced LIKELIHOOD, or a combination of them. Retention of

those risks that are below this specified threshold can be proposed automatically. Risks below the proposed threshold will be retained to be accepted without further treatment, and the rest of the options will be assessed for the risks that remain above it. For example, the Security Risk Manager (SRM) could by default propose the retention for acceptance of Risks below 6 in a range from 1-50. This threshold should be clearly recorded as part of the risk study and communicated to stakeholders. Such automatic retention should be applied after all other options have been envisaged, possibly including already retain options.

- Detailed Risk Acceptance criteria can be defined by the organisation, the System Owner or even the Security Risk Manager (SRM). If defined, such criteria must be recorded as part of the risk study. Then, the Security Risk Manager (SRM) can retain risks meeting this criteria.
- If the threshold proposed or the existing detailed Risk Acceptance Criteria is not met, the Security Risk Manager (SRM) can still retain the risk but this should be clearly recorded as an exception which must be described and justified. For example, if the costs of the Security Measures required is higher than the cost of the damage itself, the Security Risk Manager (SRM) could retain the risk and propose its acceptance. Another example is risk retained *if there is approval and commitment to take action to reduce it to an acceptable level within a defined time period*.

A detailed Risk Acceptance criteria often depend on the organisation's policies, goals, objectives and the interests of stakeholders. The following should be considered when such criteria is developed:

- *multiple thresholds, with a desired target level of risk* parameters (assets, threats, dimension, impact, type of impact, likelihood, RISK LEVEL, …);
- *the ratio of estimated profit (or other business benefit) to the estimated risk*;
- *classes of risk, e.g. risks that could result in noncompliance with regulations or laws may not be accepted, while acceptance of high risks may be allowed if this is specified as a contractual requirement*;
- *how long the risk is expected to exist, e.g. the risk may be associated with a temporary or short term activity*;
- *Business criteria*;
- *Legal and regulatory aspects*;
- *Operations*;
- *Technology*;
- *Finance*;
- *Social and humanitarian factors*.

Risks retained, possibly after several other mitigations, can be proposed to the System Owner for acceptance.

8.4.2.2 Risk sharing

This option implies that the organisation will share the risk with another party that can most effectively manage the particular risk depending on risk evaluation. It does not mean that the responsibility of the risk is transferred from the System Owner to the third party: the System Owner remains the Risk Owner (remains responsible/accountable for the risk), but the management of the risk is shared between the System Owner and the third party. *It may be possible to share the responsibility to manage risk but it is not normally possible to share the liability of an impact.*

In practice, it means that treatment options – security measures – are implemented partly by the System Owner, partly by the third party. The System Owner remain responsible for the risk, the third party become responsible for the implementation of its part of the measures. In other words, the System Owner has an "obligation of results" ("obligation de résultat") in the sense of *guaranteeing the attainment of a specific result*, while the third party has an "obligation of means" ("obligation de moyens") in the sense of *the employment of the duty of care in performing a contractual obligation*. And these contractual obligations must be formalised (e.g. by security clauses in a Service Level Agreement).

Sharing can be done by insurance *that will support the consequences, or by* sub-contracting *a partner whose role will be to monitor the information system and take immediate actions to stop an attack before it makes a defined level of damage.* Both possibilities require formalisation of relations with a third party through a contract: an insurance policy with an insurance company, a service level agreement (SLA) with an outsourcing company.

This option will be addressed in those cases in which the organisation cannot afford the potential consequences of identified risks or has a lack of the expertise or resources required to do so. This option does not include the transfer of liability arising from risks that remains on the organisation.

Risk sharing involves a decision to share certain risks with external parties. Risk sharing can create new risks or modify existing, identified risks. Therefore, additional risk treatment may be necessary.

If Risk Sharing is defined as a specific treatment option, ITSRM Methodology proposes to have the possibility to record it as such but to treat it as Risk Modification:

- Insurance will be recorded as a specific security measure (of type contractual), which mitigates only consequences by ensuring contractually the compensation of loss due to the materialisation of the risk (usually in money, could be replacement for loss of goods); the mitigation factor will depend upon the contractual clauses;
- Outsourcing will be recorded by enriching the model of the system with a Service that will be outsourced (re-use of Shared Service, see in System Modelling); that way, shared risks and measures can be imported from the service provider (from the Shared Service).

Risk sharing involves a decision to share certain risks with external parties. Risk sharing can create new risks or modify existing, identified risks. Therefore, additional risk treatment may be necessary. So, the Security Risk Manager (SRM) can have to get back to modelling and restart an iteration of risk assessment and treatment.

8.4.2.3 Risk avoidance

When the identified risks are considered too high, or the costs of implementing other risk treatment options exceed the benefits, a decision may be made to avoid the risk completely, by withdrawing from a planned or existing activity or set of activities, or changing the conditions under which the activity is operated.

For example, for risks caused by nature it may be most cost effective alternative to physically move the information processing facilities to a place where the risk does not exist or is under control. [ISO27005]

This option will be the most suitable if the benefits obtained from the activities that cause the risk are not relevant for the organisation and can be modified or abandoned, making the risk disappearing.

In practice, there are two ways to cope with risk avoidance, which are not exclusive, to keep trace of the reasoning:

- the avoidance option is recorded as such with a description of actions which need to be performed in practice (modify the system, abandon a part of the system ...). In this case, the risk remains identified and evaluated (probably high). It is when actions will be actually taken that the risk can be removed (see below);
- the Security Risk Manager (SRM) restart an iteration by modifying the model to change/remove the part of the system, or its context, which gave rise to the risk. This records the result of actions proposed for avoidance. In this case, the risk will de facto disappear from the list of identified risks, or will be recomputed lower.

8.4.2.4 Risk modification

The objective of risk modification is usually to reduce risks to an acceptable level. This is why this option is often referenced as Risk Reduction or Risk Mitigation.

As explained in [ISO27005], *the level of risk should be managed by introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable* (i.e. the Risk Acceptance Criteria is met).

During control selection it is important to weigh the cost of acquisition, implementation, administration, operation, monitoring, and maintenance of the controls against the value of the assets being protected. Furthermore, the return on investment in terms of risk reduction and potential to exploit new business opportunities afforded by certain controls should be considered.

Various constraints should be taken into account when selecting controls and during implementation. Typically, the following are considered:

- *Time constraints*
- *Financial constraints*
- *Technical constraints*
- *Operational constrains*
- *Cultural constraints*
- *Ethical constraints*
- *Environmental constraints*
- *Legal constraints*
- *Ease of use*
- *Personnel constraints*
- *Constraints for integrating new and existing controls*

The Security Risk Manager (SRM) can define iteratively Figure 8-3: Main iteration in Risk Management processes several mitigation treatments and recalculate Residual RISK LEVEL.

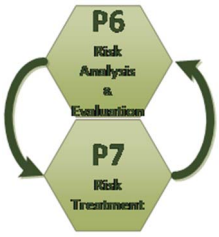


Figure 8-3: Main iteration in Risk Management processes

Step 1: The Security Risk Manager (SRM) selects a Security Measure to reduce the risk. This selection is done in the following order:

(1) select an existing Security Measure from the Security Measures Register (Security Measure that is already implemented in the Target System);
(2) select a mandatory Security Measure from the Security Measures Register (Security Measure that is mandated by constraint as identified in System Security Characterisation process);
(3) select another Security Measure already in the Security Measures Register;
(4) add a new Security Measure in the Security Measures Register, using the Catalogue of Security Measures;
(5) Create a measure or take a measure from another catalogue when it does not exist at all in the provided catalogue.

The basic rationale behind this proposed order is to optimise the effort of implementation of measures by selecting those that fulfil several requirements and/or are already implemented.

> **Note:** A Security Measure in the Measure Register is identified by the Security Measure, its Target (i.e. where it is implemented) and its Sophistication Level. A Security Measure chosen for implementation but to be applied on a different Supporting Asset or with a different Sophistication Level, should be considered as a different Security Measure in the Measure Register.

Step 2: The Security Risk Manager (SRM) identifies the location where the Security Measure will be implemented to actually mitigate the risk (i.e. define the Target of the Security Measure).

> **Note:** An implementation of a Security Measure is identified by the Security Measure, the Supporting Asset on which it is implemented and its Sophistication Level. If the measure selected in step 1 has already a Target identified which is different, a different Security Measure should be added as a different treatment in the Treatment Register.

Step 3: The Security Risk Manager (SRM) chooses a Sophistication Level for the implementation of the measure. This choice is based on the gap between the level of risk before mitigation and the expected Residual Risk after.

When selecting the Sophistication Level, the Security Risk Manager (SRM) should remind that the relation between Mitigation Factor and Sophistication Level follows a Pareto law. At Sophistication Level 1, the mitigation is already high, at relatively low cost. Going to higher level of sophistication increases the cost exponentially while the reduction increases marginally. Consequently, it is advised to always start with Sophistication Level 1, and increase it if the value of the asset that will be protected is so high that it deserves a costly measure. For example, Sophistication Level 2 could be envisaged when consequence of the risk is 4 or 5, and Sophistication Level 3 when it is higher than 5.

> **Note:** A Security Measure in the Measure Register is distinguished by the Security Measure, its Target and its Sophistication Level. If the measure selected in step 1 has already a Sophistication Level identified that is different, the Security Risk Manager (SRM) can modify the Sophistication Level but keeping in mind that this will modify it for all risks that are mitigated by the measure.

Step 4: The Security Risk Manager (SRM) assesses the Mitigation Factors for Consequence and Likelihood for the chosen Security Measure and Sophistication Level. The Extended Catalogue of Security Measures will propose these factors to help the Security Risk Manager (SRM) (see remarks in annex C.5).

> **Note:** Mitigation Factors for Consequence and Likelihood are propositions in the extended Catalogue of Security Measures: the Security Risk Manager (SRM) is free to propose different values as long as this modification is clearly flagged and justified, recorded as an exception in the current Risk Study.

Step 5: The Security Risk Manager (SRM) will link the above defined Security Measure with all identified Risks that it can mitigate. This can be done by adding the corresponding treatment in the Treatment Register. To complete this step, the Security Risk Manager (SRM) will:

- Consult the extended Catalogue of Security Measures to identify the Security Measures that apply regarding the threat, type of Supporting Asset and Security Dimension included in the risk scenario.
- Analyse the System Model to support the identification of, where, how and what Security Measures will be implemented (Target of the Security Measure).
- Read the description of the Sophistication Levels of applicable Security Measures in the extended Catalogue of Security Measures and select the most suitable to reduce risk to acceptable level.

Some risk treatments can effectively address more than one risk. Consequently, the Security Risk Manager (SRM), after proposing a treatment option for a given risk, should check if other risks might be treated with the same treatment and link them accordingly.

In Risk Modification/Mitigation option, the level of risk should be managed by introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable. This can be achieved through the application of the following actions:

A. Increase the Sophistication Levels of the Security Measures that are already implemented (this will modify all risks mitigated by the measure).
B. Implement additional Security Measures (equivalent to apply several times the mitigation option)
C. As third option the Security Risk Manager (SRM) may decide to remove implemented Security Measures and implement others that are more effective.

The selection of one option or the other will depend on the mitigation that needs to be achieved to reduce the risk to acceptable levels (to meet the Risk Acceptance Criteria). To achieve this objective, the Security Risk Manager (SRM) may combine the three options if this approach is the most effective regarding the risk reduction required, the type of Supporting Assets to be protected and the business criteria and constraints defined by the organisation.

That way, the ITSRM Methodology can be seen as a simulator of different risk treatment option to converge to an acceptable set of security measures to be implemented that would be acceptable by the decision-maker (System Owner).

8.4.3 Specific case: risk treatment when shared services are re-used

As described in the Risk Analysis process, Residual RISK LEVEL of risks imported from a Shared Service can be recalculated in the context of the using system. These are thus Residual Risks due to the treatment offered by the Shared Service.

This does not prevent the Security Risk Manager (SRM) to further mitigate these risks by adding additional Security Measures that will reduce further the Residual RISK LEVELs using the same formula on top of the imported/recalculated Residual RISK LEVEL, as long as additional measures are independent from the measures used in the Shared Service.

This requires to establish a dialogue between the Client and the Service Provider, materialised by a Service Level Agreement (SLA), which is anyway required in case of outsourcing as seen in risk sharing option.

9 OTHER RISK MANAGEMENT PROCESSES

9.1 Abstract

The current version of ITSRM Methodology does not cover in the details the implementation of the three remaining Risk Management Processes, as described in [CD46/2017]:

- Risk Acceptance – *the decision to accept the risks and responsibilities for the decision should be made and formally recorded;*
- Risk Communication and Consultation – *information about risk should be exchanged and/or shared between the decision-maker and other stakeholders;*
- Risk Monitoring and Review – *risks and their factors (i.e. assets, asset value, impact, potential adversaries, attractiveness, model, threats, frequency, easiness, measures, mitigation factors, ...) should be monitored and reviewed to identify any changes in the context of the organisation at an early stage, and to maintain an overview of the complete risk picture.*

ITSRM Methodology can be seen as a simulator that, based on the model and context of a system, provides a list of risks for the system, a list of treatment options with measures, and the Residual RISK LEVEL for the risks taking into account the list of options and measures. These are the three main outcomes (Model/Context, Residual Risks, options/measures) of a Risk Study performed following ITSRM Methodology. The Risk Study becomes the main input to the three processes mentioned above that are briefly presented hereafter.

9.2 Risk Acceptance

The risk treatment options, ending for each risk identified by Retention or Avoidance, can be proposed by the Security Risk Manager (SRM) to the System Owner, together with the Security Measures and the corresponding Residual Level of Risks.

This Risk Study (simulation) is just a proposal by the Security Risk Manager (SRM): it needs to be globally and formally accepted by the System Owner.

If the System Owner is not willing to accept the risks as presented in the Risk Study, the process can be reiterated to create different other simulations, hopefully converging toward an acceptable study.

When accepted, the simulation (Risk Study) is frozen, ending the planning phase, and becomes the base for further implementation of security (measures) in the CIS.

9.3 Risk Communication and Consultation

Risk communication is an activity to achieve agreement on how to manage risks by exchanging and/or sharing information about risk between the decision-makers and other stakeholders. The information includes, but is not limited to the existence, nature, form, likelihood, severity, treatment, and acceptability of risks.

Effective communication among stakeholders is important since this may have a significant impact on decisions that need to be made. Communication will ensure that those responsible for implementing risk management, and those with a vested interest understand the basis on which decisions are made and why particular actions are required. Communication is bi-directional.

The following communication paths should be foreseen:

- the risk study, for agreement amongst participants and for acceptance by the SO;
- the description of security measures to their implementers;
- reports on risk profiles from SO's to their Head of Department;
- information sharing between SO's and DIGIT;

- report on risk, risk management and security measures from SO's to DIGIT;
- reporting of DIGIT to ITCB on the corporate risk landscape;
- information sharing with Security Monitoring and Incident Handling capacities;
- information gathering on risk landscape.

9.4 Risk Monitoring and Review

Risks are not static. They depend on many factors that evolve in time. New threats may appear, or become more (or less) frequent. Organisation can be targeted by more powerful adversaries. The IT system will evolve technically, will process more data, potentially more valuable.

Any change in these factors will change risks, and consequently the decisions based on them.

The System Owner should ensure that the following are continually monitored:

- Organisation and System context and objectives;
- Primary Assets, their value and their Potential Adversaries;
- Supporting Assets and the (model of the) system;
- Threat landscape;
- Security incidents.

On top of the regular review, any change in these should trigger a new iteration of the Risk Management processes.

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
[IR46/2017]	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
[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
[CD844/2001]	COMMISSION DECISION of 29 November 2001amending its internal Rules of Procedure (notified under document number C(2001) 3031) (2001/844/EC, ECSC, Euratom)
[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)
[GL-AC/2014]	European Commission Information System Security Policy C(2006)–3602 - GUIDELINES ON ASSET CLASSIFICATION (Version 3 of 23/10/2014)
[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
[IR3602/2009]	IMPLEMENTING RULES FOR COMMISSION DECISION C(2006) 3602 of 16.8.2006 concerning the security of information systems used by the European Commission
[ISO27005]	International Standard ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management
[NIST SP800-53r4]	NIST Special Publication SP800-53 revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, 2015
[PM²]	PM² - Project Management Methodology – Guide 3.0 (2018)
[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
[SN1903/2019]	C(2019) 1903 final - Security Notice - Information assessment and classification

ANNEX A.2: DEFINITIONS

Asset	"Anything that has a value for the Commission" This methodology distinguishes among Primary and Supporting assets (see definitions provided in this annex).
Asset Value	Value of the asset assessed in terms of the maximum Impact (Business or Data Protection) in case of loss of a Security Dimensions (confidentiality, integrity, availability); this is also known as the Security Need.
Availability	Property of being accessible and usable upon request by an authorised entity. *(ISO/IEC 27000:2018)*
Business Manager	Role defined in [PM²] notably responsible for ensuring that the project's deliverables fulfil the business and user needs.
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)*
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities or processes. *(ISO/IEC 27000:2018)*
CONSEQUENCE	Outcome of an event affecting objectives. *(ISO/IEC 27000:2018)*
Control	"Measure that is modifying *risk*" (ISO 27000:2018) "Control is also used as a synonym to safeguard or countermeasure" (ISO 27005:2011)
Data controller	" the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (*[GDPR]*).
Data owner	"Means the individual responsible for ensuring the protection and use of a specific Data Set handled by a CIS" (*CD46/2017*).
Data Set	"Means a set of information which serves a specific business process or activity of the Commission" (*CD46/2017*).
Data Subject	A data subject is any person whose personal data is being collected, held or processed
EASINESS	Valuation of the effort required to materialise a given intentional threat. (ITSRM² v1.0)
Effectiveness	"Extent to which planned activities are realized and planned results achieved" *(ISO 27000:2016)*
Event	"Occurrence or change of a particular set of circumstances. An event can sometimes be referred to as an "incident" or "accident"." (ISO 27000:2018)
FREQUENCY	Description of the quantitative or qualitative values used to express the periodicity of accidental threats from materialising. (ITSRM² v1.0)
Function	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.
Impact	"Adverse change to the level of business objectives achieved" *(ISO/IEC 27005:2008*. The Impact definition is not included in the latest version of ISO27005 (2011).
Impact Scenario	Combination of Primary Asset, Security Dimension (C, I or A), impact type, effects, and level related to the worst case scenarios described by the organisation to determine the Primary Asset values (*ITSRM²*).
Incident	"An event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system" *(ENISA).* "An event can sometimes be referred to as an incident or accident" (ISO 27005:2011)
Inherent Risk	The Risk without taking any Security Measure into account. (ITSRM² v1.0) Inherent risk represents the amount of risk that exists in the absence of controls (FAIR Institute). Inherent risk is current Risk Level given the existing set of controls rather than the hypothetical notion of an absence of any controls (FAIR Institute) ISO does not define the notion of inherent risk but it could be defined by opposition to the notion of residual risk as: risk *existing before* risk treatment.
Integrity	Property of accuracy and completeness. *(ISO/IEC 27000:2018)*

INTEREST	The level of INTEREST of an adversary to commit a threat on a given Primary Asset. (ITSRM² v1.0)
IT Security	Preservation of confidentiality, integrity and availability of [Data Sets] Note 1: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. (paraphrasing ISO/IEC 27000:2018 for Information Security)
IT Security Event	Identified occurrence of a system, service or network state indicating a possible breach of [IT] security policy or failure of control, or a previously unknown situation that can be security relevant. (paraphrasing ISO/IEC 27000:2018 for Information Security Event)
IT Security Incident	"Event that could adversely affect the confidentiality, integrity or availability of a CIS" (*CD46/2017).* "single or a series of unwanted or unexpected [IT] security events that have a significant probability of compromising business operations and threatening [IT] security." (paraphrasing ISO/IEC 27000:2018 for Information Security incident)
IT security need	"Means a precise and unambiguous definition of the levels of confidentiality, integrity and availability associated with a piece of information or an IT system with a view to determining the level of protection required". *(CD46/2017)*
IT security risk	"Means an effect that an IT security threat might induce on a CIS. As such, an IT security risk is characterised by two factors: (1) uncertainty, i.e. the likelihood of an IT security threat to cause an unwanted event; and (2) impact, i.e. the consequences that such an unwanted event may have on a CIS" *(CD46/2017).* *"In the context of [IT] security management systems, [IT] security risks can be expressed as effect of uncertainty on [IT] security objectives." (paraphrasing ISO/IEC 27000:2018, note 5 to definition of risk)* For the context of this methodology this concept will be shortened to risk.
Level of risk	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood. *(ISO/IEC 27000:2018)*
LIKELIHOOD	Chance of something happening. *(ISO/IEC 27000:2018)*
Local Informatics Security Officer (LISO)	"Means the officer who is responsible for IT security liaison for a Commission department" *(CD46/2017).*
Mitigation Factor	Percentage of the risk (likelihood and/or consequence) that is reduced by a Security Measure. *(ITSRM²)*
Organisation	Commission Department, Directorate General or DG Unit and EU Executive Agencies owners or stakeholders of the Target System *(ITSRM²).*
Personal Data	"Processing of personal Data', 'controller' and 'personal Data filing system' shall have the same meaning as in Regulation (EC) No 45/2001, and in particular Article 2 thereof" *(CD46/2017).* Note: Regulation (EC) No 45/2001 has been repealed by Regulation (EU) 2018/1725 [IDPR] Any information relating to an identified or identifiable natural person ('data subject')
Primary asset	'For the application of this methodology this will be referred to as Data and Functions (*ITSRM²*).
Potential Adversary	Individual or group interested in provoking loss of Confidentiality, Integrity and/or Availability of any Primary Asset of the Target System. (*ITSRM²*). This concept is similar to the concept of Threat Agent often used in other methodologies. The term Threat Agent is more used in defining Risk Scenarios, as the entity which actually perform the Threat. The term Potential Adversary is used in defining Impact Scenarios, as the entity that could be interested that the threat occurs. The Potential Adversary can perform the threat him/herself, and act as a Threat Agent, or he/she can be the sponsor of another Threat Agent. In this methodology, we focus on the capacities and interest of the Potential Adversary as he/she can sponsor a Threat Agent.
POWER	Based on the combination of the Potential Adversary knowledge, its capabilities, and the resources to perform an attack successfully (*ITSRM²*).
Residual risk	The Risk which remains after mitigation by Security Measures. (ITSRM² v1.0) Residual risk is the amount of risk that remains after controls are accounted for (FAIR Institute).

	Residual risk is whatever Risk Level remain after *additional* controls are applied (FAIR Institute). Risk remaining after risk treatment. *(ISO/IEC 27000:2018)* Residual risk can also be referred to as "retained risk". (ISO 27000:2018)
Risk	Effect of uncertainty on objectives. Note 1: An effect is a deviation from the expected — positive or negative. Note 2: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. Note 3: Risk is often characterised by reference to potential "events" and "consequences", or a combination of these. Note 4: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" of occurrence. (ISO/IEC 27000:2018) For the application of this methodology the concept of risk is aligned with the definition provided for "IT security risk" shortened to risk (*ITSRM²).*
Risk acceptance	Informed decision to take a particular risk.*(ISO/IEC 27000:2018)*
Risk Acceptance Criteria	Risk acceptance criteria should be developed and specified. Risk acceptance criteria often depend on the organization's policies, goals, objectives and the interests of stakeholders. An organization should define its own scales for levels of risk acceptance. The following should be considered during development: • risk acceptance criteria may include multiple thresholds, with a desired target level of risk, but provision for senior managers to accept risks above this level under defined circumstances; • risk acceptance criteria may be expressed as the ratio of estimated profit (or other business benefit) to the estimated risk; • different risk acceptance criteria may apply to different classes of risk, e.g. risks that could result in noncompliance with regulations or laws may not be accepted, while acceptance of high risks may be allowed if this is specified as a contractual requirement; • risk acceptance criteria may include requirements for future additional treatment, e.g. a risk may be accepted if there is approval and commitment to take action to reduce it to an acceptable level within a defined time period. Risk acceptance criteria may differ according to how long the risk is expected to exist, e.g. the risk may be associated with a temporary or short term activity. Risk acceptance criteria should be set up considering the following: • Business criteria • Legal and regulatory aspects • Operations • Technology • Finance • Social and humanitarian factors *(ISO/IEC 27005:2018)* Similar to "Risk Criteria" in ISO/IEC 27000:2018
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk (also referred to as risk calculation in this methodology). Note 1: Risk analysis provides the basis for risk evaluation and decisions about risk treatment. *(ISO/IEC 27000:20186)*
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation. *(ISO/IEC 27000:20186)*
Risk avoidance	"The activity or condition that gives rise to the particular risk should be avoided." *ISO/IEC 27005:2018)*
Risk communication and consultation	Continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk. *(ISO/IEC 27000:2018)*
Risk Criteria	Terms of reference against which the significance of risk is evaluated.

	Note 1: Risk criteria are based on organizational objectives, and external and internal context Note 2: Risk criteria can be derived from standards, laws, policies (3.53) and other requirements (3.56). *(ISO/IEC 27000:2018)* Similar to "Risk Acceptance Criteria" in ISO/IEC 27005:2018
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. *(ISO/IEC 27000:2018)*
Risk identification	Process of finding, recognizing and describing risks. Note 1: Risk identification involves the identification of risk sources, events, their causes and their potential consequences. Note 2: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs. *(ISO/IEC 27000:2018)*
Risk management	Coordinated activities to direct and control an organization with regard to risk. *(ISO/IEC 27000:2018)*
Risk management process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk. *(ISO/IEC 27000:2018)*
Risk mitigation	Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction". (ISO 27000:2018)
Risk modification	The level of risk should be managed by introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable. (ISO 27005:2018)
Risk owner	Person or entity with the accountability and authority to manage a risk. *(ISO/IEC 27000:2018)*
Risk reduction	Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction". (ISO 27000:2018) "Actions taken to lessen the probability, negative consequences, or both, associated with a risk" *(ENISA).*
Risk retention	The decision on retaining the risk without further action should be taken depending on risk evaluation. (ISO 27005:2018) "Acceptance of the burden of loss or benefit of gain from a particular risk" *(ENISA).*
Risk scenario	Combination of Primary Asset, Security Dimension, Supporting Asset, and threat *(ITSRM²).*
Risk sharing	"The risk should be shared with another party that can most effectively manage the particular risk depending on risk evaluation" (ISO 27005:2018)
Risk Study	Set of information gathered and results obtained when performing the seven Processes (P1-P7) of the ITSRM Methodology. This mainly consist in: A description of the CIS and its environment (P1-P4) (Context) The risks with inherent and residual levels (P5-P6) (Risk Assessment) The security measures (P7) (Risk Treatment)
Risk transfer	Sharing with another party the burden of loss or benefit of gain, for a risk. *(ISO 27005:2008).* *Replaced with "Risk sharing" in (ISO 27005:2011)*
Risk treatment	Process to modify risk. Note 1: Risk treatment can involve: avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; taking or increasing risk in order to pursue an opportunity; removing the risk source; changing the likelihood; changing the consequences; sharing the risk with another party or parties (including contracts and risk financing); retaining the risk by informed choice. (ISO 27000:2018) Controls to reduce, retain, avoid, or share the risks should be selected and a risk

	treatment plan defined. … There are four options available for risk treatment: risk modification, risk retention, risk avoidance and risk sharing. (ISO 27005:2018) Process of selection and implementation of measures to modify risk. Risk treatment measures can include avoiding, optimising, transferring or retaining risk. *(ENISA).*
Security measure	Actionable control that can be implemented according to a priority level to mitigate a risk . (ITSRM^2 v1.0)
Security Risk Manager (SRM)	The person responsible for the ITSRMM execution.
Scale	Ordered set of values, continuous or discrete, or a set of categories to which the attribute is mapped *(ISO/IEC 27000:2016)*
Service	A service is a means of delivering data processing (Data Sets and Functions) to customers, internally or externally. An IT service is made up of a combination of Information Technology products (hardware and software), people and locations. In ITSRM Methodology, a Service is modelled as a Supporting Asset of type "service" which is itself made of a sub-set of Supporting Assets.
Shared Service	A Service is shared when its Risk Study is published, entirely or partially, by its Service Provider to be re-used in Risk Studies of CIS that are using the Service.
Stakeholders	Internal and external organisations or people with interest on the Target System Data and Functions. "Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organisation, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria" *(ISO 31000:2009)*
Sophistication Level	Scale used to measure the technical level of implementation of Security Measures *(ITSRM^2).* Depending upon its technical level of implementation (Sophistication Level), a security measure can be more or less strong, providing a more or less reduction of a risk. For example, simple password authentication and two-factor authentication could be considered as two different sophistication levels for implementing authentication.
Supporting Asset	Asset used or involved in the processing of the Data and Functions provided by the Target System. Hardware, software, personnel, locations and services are the main supporting assets that build an IT System. Supporting Assets are also known as Secondary Assets or IT Assets. *(ITSRM^2)*
System model	Representation of the architecture of the system in relation with the Supporting Assets used to manage the Data and Functions (Primary Assets) managed by the Target System. (*ITSRM^2)*
System Owner (SO)	Individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of a CIS. (*CD46/2017).*
System Security Officer (SSO)	Advises the System Owner, System Manager and Project Manager on the IT security approach and takes an active role as IT security expert to define IT security requirements and assists in the architecture, design, implementation and verification activities of IT security (*[IR46/2017]*).
Target of a Security Measure	The target of a Security Measure is the place where the measure can be actually implemented. Such target can be the organisation (e.g. a general security policy), the system (e.g. Risk Management, Code review, vulnerability scan) or a particular Supporting Asset (e.g. encryption on a data link or a hard disk, access control to an Operating System).
Target system	The specific CIS subject to the ITSRMM execution *(ITSRM^2).*
Threat	Potential cause of an unwanted incident, which may result in harm to a system or organization. *(ISO/IEC 27000:2018)*
User	Any individual who uses Functionality provided by a CIS, whether inside or outside the Commission". *(CD46/2017)*

ANNEX A.3: ACRONYMS

For the purpose of the methodology, the following acronyms have been used:

BM	Business Manager
CIA	Confidentiality, Integrity & Availability
CIS	Communication and information system
DG	Directorate General
DO	Data Owner
DPC	Data Protection Coordinator
EUCI	European Union Classified Information regulation
EC	European Commission
GDPR	European Data Protection Regulation
IDPR	Institutions Data Protection Regulation
IT	Information Technology
ITS	IT Security
ITSRM	IT Security Risk Management
ITSRM^2	IT Security Risk Management Methodology (v1.0)
LISO	Local Informatics Security Officer
MF	Mitigation Factor
MTPD	Maximum Tolerable Period of Disruption
NIST	National Institute of Standards and Technology
PA	Primary Asset
PM^2	Project Management Methodology
PII	Personal Identifiable Information
SA	Supporting Asset
SM	Security Measure
SL	Sophistication Level
SLA	Service Level Agreement
SO	System Owner
SRM	IT Security Risk Manager
SSC	System Security Characterisation
SSO	System Security Officer

ANNEX A.4: CHANGES FROM PREVIOUS VERSION

The following changes have been made between ITSRM² v1.0 (March 2018) and ITSRM Methodology v1.2 (July 2020).

Introduction	Notion of Risk Study added. (v1.2) Impact on Data Subject has been considered at same level as impact on business in the risk formula.
Process 1	Different possibilities to define and record a Risk Acceptance Criteria have been added.
Process 2	(v1.2) Data Sets that are Personal Data are flagged as such in the inventory of Primary Assets. Clarification of the notion of Primary Asset Container (was previously treated as Supporting Asset). Introduction of the notion of System Value based on Asset Value of Primary Assets the System processes. (v1.2) Asset Valuation performed by Impact Assessment is now extended to consider Impact on Data Subject (for Personal Data) and not only impact on Business. Notion of MTPD ("Maximum Tolerable Period of Disruption") has been added to take into account different unavailability periods when assessing Availability Security Dimension. Clarification on the three types of scenarios (impact, interest, and risk).
Process 3	Clarification of the notions of Service and Shared Service.
Process 4	Clarification of the notion of Service (Supporting Asset) and its use in modelling and service/risk sharing. Clarification on the use of Containers to model the interface with shared services. Details on possible Logical Model removed. Emphasize the key concept of Model in ITSRM Methodology.
Process 5	Clarification on Risk Identification when Shared Services are reused.
Process 6	Clarification on the notion of Inherent Risk. Clarification on the possibility to change provided values for Easiness and Frequency. Clarification on Risk Analysis and Evaluation when Shared Services are reused
Process 7	Clarification of the notion of target of a Security Measure. Clarification on the different Risk Treatment options, both in theory and in practice in ITSRM Methodology. Clarification on the choice of a Sophistication Level. Clarification on the possibility to change provided values for Mitigation Factors. Clarification on Risk Treatment when Shared Services are reused: additional measures.
Other Processes	Some information provided on the three processes not in scope of this version of the methodology: 1) Risk Acceptance, 2) Risk Communication and Consultation, and 3) Risk Monitoring and Review.
Annex A	(v1.2) Annex A.2: added definitions of Personal Data and Data Subject. Annex A.2: alignment of definitions with latest standards. (v1.2) Annex A.4 (Changes from previous version) has been added.
Annex B	(v1.2) Annex B.1 split into (A) Business Impact Scale, and (B) Data Protection Impact Scale. Annex B.1: a mapping between ITSRM² Business Impact Scale (0-10) and scale proposed in former framework (1-5) has been provided into (C), with a mapping on former and current information classification levels. (v1.2) Annex B.3 added to map likelihood scales between ITSRM² and DPIA
Annex C	Annex C.5: All measures from NIST SP800-53r4 have been added but split into 1) Mitigating measures, 2) Supporting Measures, and 3) Corporate Measures. Link between Supporting Measures and their supported Mitigating Measures has been explicated. Rationale has been provided for definition of Mitigation Factors. Mechanism of "exception": freedom to change values provided in extended catalogues. New family (Legal and Financial protection) and new measure injected in the (NIST) catalogue of measures to cope with some treatment options.

ANNEX A.5: GLOBAL RASCI TABLE

	SO	DO	LISO	DPC	SRM	IT Staff	HoD
P1 – System Security Characterisation							
System Description	R	-	S	C	R(D)	-	A
Identification of Security-related Roles	R	-	S	-	R(D)	-	A
Organisation Description	R	-	S	-	R(D)	-	A
Identification of Main Constraints	R	-	S	-	R(D)	-	A
Identification of Mandatory Security Measures	R	-	S	C	R(D)	-	A
P2 – Primary Assets							
Primary Asset Identification	R	S	C	C	R(D)	S	A
Asset Valuation	R	S	C	C	R(D)	-	A
Primary Asset Attractiveness Valuation	R	S	C	C	R(D)	-	A
P3 – Supporting Assets							
Supporting Asset Identification	R	-	C	-	R(D)	S	A
P4 – System Modelling							
System Modelling	R	I	C	-	R(D)	S	A
P5 – Risk Identification							
Risk Identification	R	I	C	I	R(D)	C	A
Existing Security Measures Identification	R	I	S	I	R(D)	S	A
P6 – Risk Analysis & Evaluation							
Risk Analysis	R	-	-	-	R(D)	-	A
Risk Evaluation	R	I	C	C	R(D)	I	A
P7 – Risk Treatment							
Selection of Risk Treatment Options	R	I	C	C	R(D)	-	A
Detailing the Treatment	R	I	C	C	R(D)	C	A

ANNEX B.1A: IMPACT SCALE (BUSINESS IMPACT)

		Impact level (I)				
Impact value	***0***	***1***	***2***	***3***	***4***	***5***
Impact type						
Financial loss (in %age of EC budget)		< 0.001%	0.001% to 0.01%	0.01% to 0.05%	0.05% to 0.5%	0.5% to 2%
Financial loss (based on 3.5G€ Functioning budget of the EC)		< 50.000€	50.000€ to 500.000€	500.000€ to 2M€	2M€ to 20M€	20M€ to 100M€
Delay in political decision / execution		One week or negligible delay	Two weeks delay	One month or moderate delay	Two months delay	Four months delay
Damage political relations		Negligible damage to relations with Commission's partners.	Moderate damage to relations with Commission's partners	Consequential damage to political relation with Commission's partners	Significant damages adversely affecting relations with Commission's partners	Serious damages to relations with Commission's partners
Result in critical intervention at political level (Council/Parliament) regarding the Commission's performance		Minimum intervention	Minimum intervention with some resolution via alternative routine operations	Moderate intervention	Moderate intervention with substantial resolution via alternative routine operations	Consequential, affects execution of political decisions
Degradation of the Commission services (delayed delivery, %age of expected time)		1% delay		10% delay		25% delay
Disruption of activities		Could cause disruption to activities within the EC		Is likely to cause disruption to activities within the EC		Is likely to cause disruption to activities within the EC and with impact on other organisations
Damage to health and safety		Minor injury(ies) to one individual	Minor injury(ies) to some individuals	More than minor injuries to several individuals	Injuries to several individuals	Major injuries or widespread injuries
Damage to Staff morale and productivity		Negligible	Minimum	Moderate	Consequential	Significant
Damage to Organisation image and reputation		Negligible damage to image and reputation	Moderate negative publicity, limited to local/specific public	Consequential, limited to local/specific public	Moderate negative publicity, to general public	Consequential or limited to 3 EU countries
Damage to Public Order		Negligible impact, no disruption to community	Limited or very localised protest	Some alteration to public order	Limited or very localised protest, endangering individual security or liberty	Consequential, region wide protest, lightly injured people
Infringement of Laws and regulation		No relevant legal consequences for the **EC**	No relevant legal consequences for the EC or third parties.	Internal legal consequences for the EC	Internal legal consequences that include fines and economic penalties for the EC	

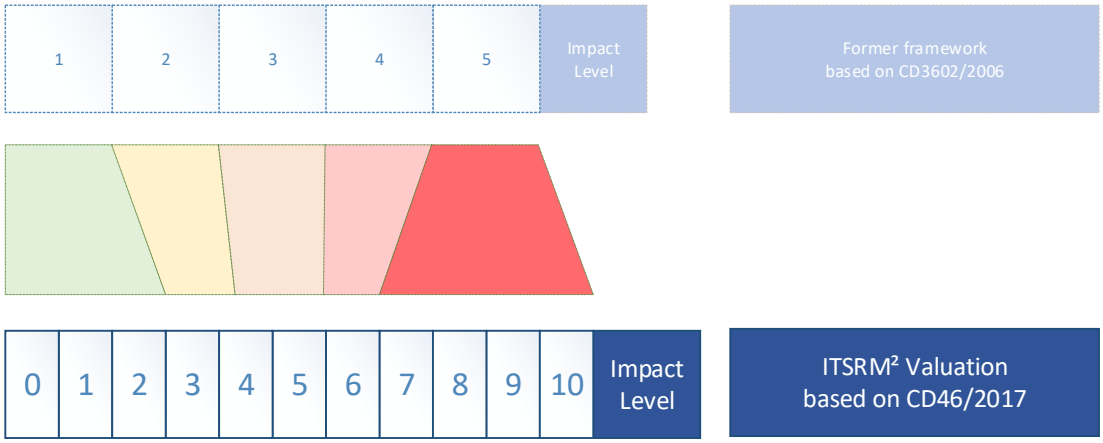
	Impact level (II)				
Impact value	***6***	***7***	***8***	***9***	***10***
Impact type					
Financial loss (in %age of EC budget)	2% to 5%	5% to 30%	30% to 200%	200% to 1000%	> 1000%
Financial loss (based on 3.5G€ Functioning budget of the EC)	100M€ to 250M€	250M€ to 1.5G€	1.5G€ to 10G€	10G€ to 50G€	> 50G€
Delay in political decision / execution	Six months or significant delay	One year delay	Two years delay	Four years delay	Abandoned execution
Damage political relations	Significant damages affecting political relations in Member States	Serious; raise tension or formal protest in some Member States	Serious; raise tension or formal protest in several Member States	Exceptionally grave; raise tension or formal protest in the EU and with others countries.	Termination of relations between EU commission and member state or strategic alliance partner
Result in critical intervention at political level (Council/Parliament) regarding the Commission's performance	Significant or impede important executions	Serious, disrupt execution(s)	Serious, disrupt execution(s) with disablement of execution of political decisions	Exceptionally grave, abort critical execution(s)	Stopping significant number of execution(s) with disablement of execution of political decisions
Degradation of the Commission services (delayed delivery, %age of expected time)	50% delay				
Disruption of activities	Is likely to have some impact to other organizations	Is likely to cause major impact on other organisations	Is likely to cause a serious impact on other organizations		
Damage to health and safety	Life of individual(s) threatened	Death of one individual	Death of several individuals	Permanent incapacitating injury or illness to many individuals that may lead to widespread loss of life	Widespread loss of life
Damage to Staff morale and productivity	Adversely affected	Serious loss	Complete loss		
Damage to Organisation image and reputation	Significant or limited to 5 EU countries	More than serious, Europe wide or worldwide negative publicity			
Damage to Public Order	Demonstrations national effects or injured people	Threaten stability	Serious prejudice public order/extensive disruptions on national level	Serious prejudice public order/extensive disruptions on several national levels	Widespread effects/ individual or loss of lives
Infringement of Laws and regulation	Legal consequences that include sentences of imprisonment for members of the EC	Legal consequences that affect the formal constitution of the EC			

ANNEX B.1B: IMPACT SCALE (DATA PROTECTION IMPACT PART, WITH MAPPING TO DPIA)

ITSRMM Impact Level		DPIA Severity Level
1	*Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).*	***1***
2	*Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties **(**extra costs**,** denial of access to business services, fear, lack of understanding, **stress, minor physical ailments, etc.).***	***2***
4	*Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties **(**misappropriation of funds, blacklisting by banks**,** property damage, loss of employment**,** subpoena, worsening of health, etc.).*	***3***
8	*Individuals may encounter significant**,** or even irreversible**,** consequences, which they may not overcome (financial distress such as substantial debt or inability to work**,** long-term psychological or physical ailments**,** death**, etc.).***	***4***

ANNEX B.1C: IMPACT SCALE (MAPPING WITH OTHER FRAMEWORKS)

Previous framework for IT security, based on Commission Decision 3602(2006), proposed, in a guideline for asset classification, an impact scale with five levels. To ease migration from this former framework, the Security Risk Manager (SRM) can use the equivalence proposed below.



The rationale behind building this scale is based on the following ideas:

- backward compatibility with former framework (similar values for levels with mapping explained above);
- keeping a logarithmic scale to clarify and ease choice of a level;
- adding zero to explicitly cope with absence of requirement;
- split of the scale into two parts:
  - first one for impacts mainly on the organisation, impacts the organisation can cope with;
  - second one for impacts going beyond the organisation itself, impact from which the organisation would have few or no chance to "survive";
- more levels in both parts for better granularity in both aspects.

Based on this equivalence between the two Impact Scales, the following mappings can be proposed with:

- former classification levels, from [CD844/2001][10], [IR3602/2009][11] and [GL-AC/2014][12], and with
- current classification levels, from [CD444/2015][13], [CD443/2015][14] and [SN1903/2019][15].

Former		ITSRM Methodology	Current
Classification	**Valuation**		**Classification**
Level	**Impact Level**		**Level**
Public	1	0	Publicly available (PA)
		1	Commission use (CU)
		2	
Limited Basic	2	3	Sensitive Non Classified (SNC)
Limited High	3	4	
		5	
RESTREINT UE / EU RESTRICTED	4	6	RESTREINT UE / EU RESTRICTED
CONFIDENTIEL UE / EU CONFIDENTIAL SECRET UE/EU SECRET TRES SECRET UE/EU TOP SECRET	5	7	CONFIDENTIEL UE / EU CONFIDENTIAL SECRET UE/EU SECRET TRES SECRET UE/EU TOP SECRET
		8	
		9	
		10	

Former		ITSRM Methodology	Current	
Integrity / Availability	**Valuation**		**Integrity / Availability**	
Level	**Impact Level**		**Level**	**Rating**
Moderate	1	0	1	Very Low
		1		
		2		
	2	3	2	Low
Critical	3	4		
		5	3	Medium
	4	6		
Strategic	5	7	4	High
		8		
		9	5	Very High
		10		

[10] COMMISSION DECISION of 29 November 2001amending its internal Rules of Procedure (notified under document number C(2001) 3031) (2001/844/EC, ECSC, Euratom)

[11] IMPLEMENTING RULES FOR COMMISSION DECISION C(2006) 3602 of 16.8.2006 concerning the security of information systems used by the European Commission

[12] European Commission Information System Security Policy C(2006) 3602 - GUIDELINES ON ASSET CLASSIFICATION (Version 3 of 23/10/2014)

[13] COMMISSION DECISION (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information

[14] COMMISSION DECISION (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission

[15] C(2019) 1903 final - Security Notice - Information assessment and classification

ANNEX B.2: INTEREST LEVEL SCALE

The concept of INTEREST relates to the extent of the efforts required by the Potential Adversary to achieve the disclosure, modification or unavailability of the Primary Assets. The values provided are determined to keep the scale form 1-5 used in all processes to ease the risk calculation.

Level	Description	Interest Value
High	**Targeting**: The Potential Adversary is determined to compromise the relevant Security Dimension of the Primary Asset and will spend significant effort to achieve that objective	**5**
Medium	**Opportunistic**: The Potential Adversary will not spend effort to compromise relevant Security Dimension of the Primary Asset, but if at the time of an attack the Potential Adversary discovers that it can be achieved with little additional effort, the Adversary will attempt it.	**3**
Low	**Non-targeting**: The damage is caused as side effect of actions targeting other Assets.	**1**

ANNEX B.3: SCALES FOR LIKELIHOOD, FREQUENCY, EASINESS

Level			Likelihood		Ease		Frequency (ARO)	
5	VH	very high	AC	almost certain	E	easy	**100**	Every day
4	H	high	VH	very high	M	medium	**10**	Every month
3	M	medium	P	possible	D	difficult	**1**	Once a year
2	L	low	U	unlikely	VD	very difficult	**0.1**	Once in 10 years
1	VL	very low	VR	very rare	ED	extremely difficult	**0.01**	Once in a century

ARO - Annual Rate of Occurrence

Mapping with DPIA likelihood

ITSRMM Level			DPIA Likelihood	
5	VH	very high	4	*Very often. Materialization of the risk is expected.*
4	H	high	3	*Quite often. Materialization of the risk would not be uncommon, but it is not certain.*
3	M	medium		
2	L	low	2	*May happen. Materialization of the risk would be uncommon or unusual, but the risk may materialize.*
1	VL	very low	1	*Rare. Materialization of the risk would be very uncommon or very unusual, cannot be excluded but the risk normally should not materialize.*

ANNEX C.1: CATALOGUE OF CONSTRAINTS TYPES

Constraints for risk treatment
Time
Financial
Technical
Operational
Cultural
Ethical
Environmental
Legal
Ease of use
Personnel
Integrating new and existing controls
Constraints for the organisation
Political nature
Strategic nature
Territorial
Economic and political climate
Structural
Functional
Concerning personnel
From the organization's calendar
Related to methods
Cultural nature
Budgetary
From pre-existing processes
Technical
Organizational

Source: ISO 27005

ANNEX C.2: CATALOGUE OF POTENTIAL ADVERSARY TYPES

Type	Subtype	Description	POWER value
External	Nation States	State-sponsored espionage activities related with intelligence or military groups, having advanced technical and operational capabilities, deep resources and patience.	5
	Cybercriminals	Organised groups that commit illegal activities involving a computer or network-connected device, e.g.: crimes in which the computing device is the target; crimes in which the computer is used as a weapon.	4
	Cyber terrorist	Hacker groups that, acting with terrorist objectives (ISIS cyber terrorist), use available anonymous tools and techniques or other illicit resources for communicating purposes, such as the deep web.	3
	Corporations	Corporate-sponsored espionage activities, usually motivated by commercial interests.	3
	Hacktivists	People that use the same tools and techniques as a hacker with the intention of disrupting services and bringing attention to a political or social cause.	2
	Script Kiddies	Individuals with very few technical knowledge and no financial, personal or ideological aspirations. They normally act by curiosity and for bragging.	1
Internal	Partner / Contractor	Organisation or individual (with no direct contractual link) that provides services to the target organisation. This may be a hosting facility, cloud provider, or any other service provider.	5
	Privileged insider	Current employee with limited knowledge about system misuses or safeguards but with privileged access to sensitive information.	5
	Insider	Current employee with limited knowledge about system misuses or safeguards and limited access to sensitive information.	3

ANNEX C.3: CATALOGUE OF SUPPORTING ASSET TYPES

Level1	Level 2	Level 3	Example
Software			
	End-user Application/module		
	Middleware		
		Web Browser	
		Web Server	
		Application server	
		DB Server	
		Network Stack	
		Operating System	
		Hypervisor	Virtualization layer
	Firmware		BIOS, ...
Hardware			
	End-point		
		Portable	Laptop, netbook, tablet, smartphone, smartcard, hard token, ...
		Fixed	Desktop, Workstation, ...
	Server		Server, Multi-purpose devices (networked printer/copier/scanner with storage), SAN, NAS, backup/storage robot, ...
	Network node		router, switch, bridge, gateway, hub, repeater, modem, Wifi Access Point
	Network media		
		Wired	Copper cable, coaxial cable, twisted pair, optical fiber, ...
		Wireless	Wifi, 801.11, Bluetooth, IR, Radio, satellite ...
	Data media		
		Digital	Hard-disk, floppy-disk, CD, DVD, USB device, tapes, cartridge, memory card, ...
		Non-digital	Paper, (micro)film, slides, ...
	Peripherals		Printing equipment, reader/writer equipment, scanning equipment, keyboard, mouse, console, screen, ...
Personnel			
	Normal user		
	Privileged user / Manager		
	Service provider		
	System supplier		
Service			
	Data Center		
		Hosting	
		Housing	
	Network services		Internet, LAN, MAN, WAN, Wifi, ADSL, X.25, ISDN, ...
	Cloud services		
		IaaS	(Infrastructure as a Service)
		PaaS	(Platform as a Service)
		SaaS	(Software as a Service)
Location / Installation			
	Area		
	Building		
	Room		Office, computer room, ...
	Physical Container		Box, cupboard, safe, rack, ...
	Mobile plateform		car, truck, bus, train, plane, ship, ...

ANNEX C.4: CATALOGUE OF THREATS

		Security Dimension			Intentional	
Label	**Threat / Type**	**[C]**	**[I]**	**[A]**	**No**	**Yes**
[N]	**Natural**					
[N.1]	Fire			x	x	
[N.2]	Water			x	x	
[N.*]	Other natural disasters			x	x	
[I]	**Industrial**					
[I.1]	Fire			x	x	x
[I.2]	Water			x	x	x
[I.*]	Other industrial disasters			x	x	x
[I.3]	Environmental pollution			x	x	x
[I.4]	Electromagnetic pollution			x	x	x
[I.5]	Hardware or software failure			x	x	x
[I.6]	Power interruption			x	x	x
[I.7]	Unsuitable temperature or humidity conditions			x	x	x
[I.8]	Communications services failure			x	x	x
[I.9]	Interruption of other services or essential supplies			x	x	x
[I.10]	Media degradation			x	x	x
[I.11]	Electromagnetic emanations	x			x	x
[E]	**Errors and unintentional failures**					
[E.1]	User errors	x	x	x	x	
[E.2]	System / Security administrator errors	x	x	x	x	
[E.3]	Monitoring errors (log)		x		x	
[E.4]	Configuration errors		x		x	
[E.7]	Organisational deficiencies			x	x	
[E.8]	Malware diffusion	x	x	x	x	
[E.9]	[Re-]routing errors	x			x	
[E.10]	Sequence errors		x		x	
[E.15]	Accidental alteration of the information		x		x	
[E.18]	Destruction of information			x	x	
[E.19]	Information leaks	x			x	
[E.20]	Software vulnerabilities	x	x	x	x	
[E.21]	Defects in software maintenance / updating		x	x	x	
[E.23]	Defects in hardware maintenance / updating			x	x	
[E.24]	System failure due to exhaustion of resources			x	x	
[E.25]	Equipment loss	x		x	x	
[E.28]	Staff shortage			x	x	
[A]	**Wilful attacks**					
[A.3]	Manipulation of activity records (log)		x			x
[A.4]	Manipulation of the configuration files	x	x	x		x
[A.5]	Masquerading of identity	x	x			x
[A.6]	Abuse of access privileges	x	x	x		x
[A.7]	Misuse	x	x	x		x
[A.8]	Malware diffusion	x	x	x		x
[A.9]	[Re-]routing of messages	x				x
[A.10]	Sequence alteration		x			x
[A.11]	Unauthorised access	x	x			x
[A.12]	Traffic analysis	x				x
[A.13]	Repudiation (denial of actions)		x			x
[A.14]	Eavesdropping	x				x
[A.15]	Deliberate alteration of information		x			x
[A.18]	Destruction of information			x		x
[A.19]	Disclosure of information	x				x
[A.22]	Software manipulation	x	x	x		x
[A.23]	Hardware manipulation	x		x		x
[A.24]	Denial of service			x		x

[A.25]	Theft	x		x		x
[A.26]	Destructive attack			x		x
[A.27]	Enemy over-run	x		x		x
[A.28]	Staff shortage			x		x
[A.29]	Extortion	x	x	x		x
[A.30]	Social engineering	x	x	x		x
[SR]	**Service-related Threats (Cloud services, services provided by 3rd parties)**					
[SR.1]	Lock-in			x	x	
[SR.2]	Loss of governance	x	x	x	x	x
[SR.7]	Isolation failure	x	x	x	x	x
[SR.9]	Management interface compromise			x	x	x
[SR.11]	Insecure or ineffective deletion of data	x			x	x
[SR.14]	Compromise of Service Engine	x	x	x	x	x
[SR.19]	Subpoena and e-discovery	x		x	x	
[SR.20]	Risk from changes of jurisdiction	x		x	x	
[SR.21]	Data protection risks	x				x
[SR.31]	Accountability and Data Ownership			x	x	x
[SR.32]	User Identity Federation			x	x	
[SR.35]	User Privacy and Secondary Usage of Data	x				x
[SR.38]	Incidence Analysis and Forensic Support	x	x	x	x	x
[SR.53]	Insecure Interfaces and APIs	x	x	x	x	x

Source: Magerit / PILAR and ENISA / OWASP / CSA (for Cloud related threats)

Remark 1: Extended Catalogue

This annex contains the list of proposed threats with basic information: the Security Dimension(s) at stake, and whether the threat is intentional and/or accidental.

An Extended Catalogue will be provided in an additional document and/or in the tool proposed to automate Risk Study. This Extended Catalogue will provide details on each Threat and will propose values for FREQUENCY and/or EASINESS of the threat. These proposals are to be used to calculate the LIKELIHOOD of the risk and consequently the RISK LEVEL (in P6 – Risk Analysis).

Remark 2: Mechanism of exception

Values for FREQUENCY and/or EASINESS of a threat are only proposals. If no value is proposed, or if the Security Risk Manager (SRM) do not agree with the proposal, he/she has the freedom to propose and use a better value based on his/her experience or preferred source.

In this case, such "exception" should simply be flagged, justified (rationale, source, …) and new value proposed following scale proposed in annex B.3.

ANNEX C.5: CATALOGUE OF SECURITY MEASURES

The catalogue proposed in the ITSRM Methodology is based on the list of security measures described by the NIST (National Institute of Standards and Technology, a unit of the U.S. Commerce Department) in its Special Publication SP800-53 revision 4 [NIST SP800-53r4] (*Security and Privacy Controls for Federal Information Systems and Organizations*, 2015).

To simplify the process of Risk Treatment, measures in this list have been regrouped, to obtain a manageable granularity, and assembled into three main categories, to ease referencing:

- Mitigating Measures that directly mitigate risks, by reducing its likelihood and/or consequence;
- Supporting Measures that indirectly mitigate risks by supporting Mitigation Measures;
- Corporate Measures that globally reduce risks when applied at the level of the organisation, not on a specific system.

Important Remark

The grouping into "mitigating", "supporting" and "corporate" measures, as well as the links supported/supporting between measures is a simple, flat, proposal which should fit a majority of the cases.

But there are situations where the Security Risk Manager (SRM) will have to adapt both grouping and interlinks. Some mitigating measures can in some circumstances be supporting of others. And the Security Risk Manager (SRM) could want to emphasise the importance of a supporting measure by consider it as a mitigating one. All these modifications are valid as long as interlinked measures in a given context are always considered as a monolithic group of measures so that:

1. the mitigation (factor) can only be applied if all interlinked measures are implemented (e.g you have good encryption if and only if you have good key management);
2. the mitigation (factor) can only be applied once for such group and not several times for several of its constituting measures (e.g. you do not have a reduction by good encryption and a second reduction by good key management).

The grouping proposed in this annex should tackle a majority of situations, but the Security Risk Manager (SRM) should always check and adapt dependencies if a specific context requires it.

Mitigating Measures

Mitigating measures directly mitigate risks, by reducing likelihood and/or consequence of the threat which gives rise to the risk. Consequently, mitigating measures will have (not null) Mitigation Factor(s).

Mitigating measures are supported by other measures. This means that a mitigating measure will be effective if and only if its supporting measures are also implemented. It is considered that supporting measures do not mitigate directly a risk, but are necessary for its mitigating measure to actually reduce the risk.

For example, encryption [SC-13] is supported by appropriate key management [SC-12]. Key management alone does not mitigate a risk, but encryption without appropriate key management will not be effective mitigating the risk.

This simplifies the Risk Treatment process as the Security Risk Manager (SRM) just needs to select measures in the subset of mitigating measures, counting on the fact that all appropriate sub-measures, including the supporting measures, will be implemented.

Their **target**, that it to say the place where they apply, is usually either:

- the **System** itself (e.g. defining a system security plan [PL-2] for a system, performing a Vulnerability Scanning [RA-5] on a system, or applying a Secure System Development Life-Cycle [SA-3]);

- a distinct **Supporting Asset** of the system (e.g. Security Awareness [AT-2] is raised on people, encryption [SC-13] is performed on a hard disk, a USB key or a communication line).

Compared to the NIST Special Publication, only one measure has been added to the ITSRM Methodology catalogue of Security Measures: [LF-2] INSURANCE CONTRACT, in the also created family [LF] Legal and Financial protection.

The Mitigation Factor for this new measure, acting on CONSEQUENCE only, will have to be determined by the Security Risk Manager (SRM) based on the specificities of the contract itself.

This measure has been created also to cope with the "Risk Sharing" risk treatment option. In the case this option concern insurance (and not outsourcing), the Security Risk Manager (SRM) can just modify/mitigate the risk by adding this [LF-2] measure to lower the risk.

Supporting Measures

It is considered that Supporting measures do not mitigate directly a risk. But if they are not implemented, the measures they support will not be effective and will not mitigate the risk. This is reflected, in practice, in the fact that the Mitigation Factor for a supporting measures is hard to define, if not possible.

For example, management of users [AC-2] and by prior user identification and authentication [IA-xx] support logical access control [AC-3]. Management of users alone does not mitigate a risk, but access control without appropriate management of users will not be effective mitigating the risk.

The Security Risk Manager (SRM) does not need to implicitly select a Supporting measure but can focus on mitigating measures, counting on the fact that this means de facto implementation of its supporting measures.

A Security Risk Manager (SRM) could decide to anyway select for treatment a supporting measure, for example to emphasise the necessity to implement it, or to clarify a particular context. In such case, the Security Risk Manager (SRM) will have to provide and justify the Mitigation Factor of the Supporting measure selected for risk reduction.

Corporate Measures

Corporate measures are measures applicable at the level of the organisation, and not specifically for a system. As such, they have not been considered neither as Mitigating measures, neither as supporting measures. Usually, such measures are implemented for the organisation, and not specifically in the context of a given system.

But similarly to Supporting measures, Corporate measures can be selected by a Security Risk Manager (SRM), for example to emphasise the necessity to implement it for the given system, or to clarify a particular context. In such case, the Security Risk Manager (SRM) will have to provide and justify the Mitigation Factor of the Corporate measure selected for risk reduction.

C.5 (1) Mitigating Measures

NAME	TITLE	is supported by
AC	Access Control	
AC-3	ACCESS ENFORCEMENT	AC-2, AC-5, AC-6, AC-7, AC-8, AC-9, AC-10, AC-11, AC-12, AC-14, AC-16, AC-22, AC-24, AC-25, IA-xx
AC-4	INFORMATION FLOW ENFORCEMENT	
AC-17	REMOTE ACCESS	AC-2, AC-5, AC-6, AC-7, AC-8, AC-9, AC-10, AC-11, AC-12, AC-14, AC-16, AC-22, AC-24, AC-25, IA-xx
AC-18	WIRELESS ACCESS	AC-2, AC-5, AC-6, AC-7, AC-8, AC-9, AC-10, AC-11, AC-12, AC-14, AC-16, AC-22, AC-24, AC-25, IA-xx
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	AC-2, AC-5, AC-6, AC-7, AC-8, AC-9, AC-10, AC-11, AC-12, AC-14, AC-16, AC-22, AC-24, AC-25, IA-xx
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	
AC-21	INFORMATION SHARING	
AC-23	DATA MINING PROTECTION	
AT	Awareness and Training	
AT-2	SECURITY AWARENESS TRAINING	AT-4
AT-3	ROLE-BASED SECURITY TRAINING	AT-4
AU	Audit and Accountability	
AU-2	AUDIT EVENTS	AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-11, AU-12, AU-14, AU-15, AU-16
AU-10	NON-REPUDIATION	AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-11, AU-12, AU-14, AU-15, AU-16
AU-13	MONITORING FOR INFORMATION DISCLOSURE	AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-11, AU-12, AU-14, AU-15, AU-16
CA	Security Assessment and Authorization	
CA-2	SECURITY ASSESSMENTS	CA-5, CA-6, CA-7
CA-3	SYSTEM INTERCONNECTIONS	
CA-8	PENETRATION TESTING	
CA-9	INTERNAL SYSTEM CONNECTIONS	
CM	Configuration Management	
CM-2	BASELINE CONFIGURATION	CM-3, CM-4, CM-5, CM-6, CM-7
CM-9	CONFIGURATION MANAGEMENT PLAN	
CM-10	SOFTWARE USAGE RESTRICTIONS	
CM-11	USER-INSTALLED SOFTWARE	
CP	Contingency Planning	
CP-2	CONTINGENCY PLAN	CP-3, CP-4
CP-6	ALTERNATE STORAGE SITE	
CP-7	ALTERNATE PROCESSING SITE	
CP-8	TELECOMMUNICATIONS SERVICES	
CP-9	INFORMATION SYSTEM BACKUP	CP-10
CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS	
CP-12	SAFE MODE	
CP-13	ALTERNATIVE SECURITY MECHANISMS	
IA	Identification and Authentication	
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	IA-4, IA-5, IA-6, IA-7, IA-10, IA-11
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	IA-4, IA-5, IA-6, IA-7, IA-10, IA-11
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	IA-4, IA-5, IA-6, IA-7, IA-10, IA-11
IA-9	SERVICE IDENTIFICATION AND AUTHENTICATION	IA-4, IA-5, IA-6, IA-7, IA-10, IA-11
IR	Incident Response	
IR-4	INCIDENT HANDLING	IR-2, IR-3, IR-5, IR-6, IR-7, IR-8, IR-9, IR-10
MA	Maintenance	
MA-6	TIMELY MAINTENANCE	MA-2, MA-3, MA-4, MA-5
MP	Media Protection	
MP-2	MEDIA ACCESS	MP-3, MP-4, MP-5, MP-8
MP-6	MEDIA SANITIZATION	MP-3, MP-4, MP-5, MP-8
MP-7	MEDIA USE	MP-3, MP-4, MP-5, MP-8
PE	Physical and Environmental Protection	
PE-3	PHYSICAL ACCESS CONTROL	PE-2, PE-6, PE-8, PE-16

PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	PE-2, PE-6, PE-8
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	PE-2, PE-6, PE-8
PE-9	POWER EQUIPMENT AND CABLING	PE-10, PE-11, PE-12
PE-13	FIRE PROTECTION	
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	
PE-15	WATER DAMAGE PROTECTION	
PE-17	ALTERNATE WORK SITE	
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	
PE-19	INFORMATION LEAKAGE	
PE-20	ASSET MONITORING AND TRACKING	
PL	**Planning**	
PL-2	SYSTEM SECURITY PLAN	PL-4, PL-7, PL-8, PL-9, RA-2, RA-3
PS	**Personnel Security**	
PS-2	POSITION RISK DESIGNATION	PS-5
PS-3	PERSONNEL SCREENING	PS-5
PS-4	PERSONNEL TERMINATION	PS-5
PS-6	ACCESS AGREEMENTS	PS-5
PS-7	THIRD-PARTY PERSONNEL SECURITY	PS-2, PS-3, PS-4, PS-6, PS-8
RA	**Risk Assessment**	
RA-5	VULNERABILITY SCANNING	
RA-6	TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY	
SA	**System and Services Acquisition**	
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	SA-2, SA-5, SA-8, SA-10, SA-11, SA-13, SA-15, SA-16, SA-17, SA-20, SA-21, SI-10, SI-11, SI-13, SI-15, SI-16, SI-17
SA-4	ACQUISITION PROCESS	SA-22
SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	
SA-12	SUPPLY CHAIN PROTECTION	SA-14, SA-19
SA-18	TAMPER RESISTANCE AND DETECTION	
SC	**System and Communications Protection**	
SC-2	APPLICATION PARTITIONING	
SC-3	SECURITY FUNCTION ISOLATION	
SC-4	INFORMATION IN SHARED RESOURCES	
SC-5	DENIAL OF SERVICE PROTECTION	
SC-6	RESOURCE AVAILABILITY	
SC-7	BOUNDARY PROTECTION	
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	SC-12, SC-17, SC-20, SC-21, SC-22
SC-10	NETWORK DISCONNECT	
SC-11	TRUSTED PATH	
SC-13	CRYPTOGRAPHIC PROTECTION	SC-12, SC-17
SC-18	MOBILE CODE	
SC-23	SESSION AUTHENTICITY	
SC-28	PROTECTION OF INFORMATION AT REST	SC-12, SC-17
SC-31	COVERT CHANNEL ANALYSIS	
SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	
SC-39	PROCESS ISOLATION	
SC-40	WIRELESS LINK PROTECTION	SC-12, SC-17
SI	**System and Information Integrity**	
SI-2	FLAW REMEDIATION	
SI-3	MALICIOUS CODE PROTECTION	
SI-4	INFORMATION SYSTEM MONITORING	
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	
SI-14	NON-PERSISTENCE	
LF	**Legal and Financial protection**	
LF-2	INSURANCE CONTRACT	

C.5 (2) Supporting Measures

NAME	TITLE	supports
AC	**Access Control**	
AC-2	ACCOUNT MANAGEMENT	AC-3, AC-17, AC-18, AC-19
AC-5	SEPARATION OF DUTIES	AC-3, AC-17, AC-18, AC-19
AC-6	LEAST PRIVILEGE	AC-3, AC-17, AC-18, AC-19
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	AC-3, AC-17, AC-18, AC-19
AC-8	SYSTEM USE NOTIFICATION	AC-3, AC-17, AC-18, AC-19
AC-9	PREVIOUS LOGON (ACCESS) NOTIFICATION	AC-3, AC-17, AC-18, AC-19
AC-10	CONCURRENT SESSION CONTROL	AC-3, AC-17, AC-18, AC-19
AC-11	SESSION LOCK	AC-3, AC-17, AC-18, AC-19
AC-12	SESSION TERMINATION	AC-3, AC-17, AC-18, AC-19
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	AC-3, AC-17, AC-18, AC-19
AC-16	SECURITY ATTRIBUTES	AC-3, AC-17, AC-18, AC-19
AC-22	PUBLICLY ACCESSIBLE CONTENT	AC-3, AC-17, AC-18, AC-19
AC-24	ACCESS CONTROL DECISIONS	AC-3, AC-17, AC-18, AC-19
AC-25	REFERENCE MONITOR	AC-3, AC-17, AC-18, AC-19
AT	**Awareness and Training**	
AT-4	SECURITY TRAINING RECORDS	AT-2, AT-3
AU	**Audit and Accountability**	
AU-3	CONTENT OF AUDIT RECORDS	AU-2, AU-10, AU-13
AU-4	AUDIT STORAGE CAPACITY	AU-2, AU-10, AU-13
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	AU-2, AU-10, AU-13
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	AU-2, AU-10, AU-13
AU-7	AUDIT REDUCTION AND REPORT GENERATION	AU-2, AU-10, AU-13
AU-8	TIME STAMPS	AU-2, AU-10, AU-13
AU-9	PROTECTION OF AUDIT INFORMATION	AU-2, AU-10, AU-13
AU-11	AUDIT RECORD RETENTION	AU-2, AU-10, AU-13
AU-12	AUDIT GENERATION	AU-2, AU-10, AU-13
AU-14	SESSION AUDIT	AU-2, AU-10, AU-13
AU-15	ALTERNATE AUDIT CAPABILITY	AU-2, AU-10, AU-13
AU-16	CROSS-ORGANIZATIONAL AUDITING	AU-2, AU-10, AU-13
CA	**Security Assessment and Authorization**	
CA-5	PLAN OF ACTION AND MILESTONES	CA-2
CA-6	SECURITY AUTHORIZATION	CA-2
CA-7	CONTINUOUS MONITORING	CA-2
CM	**Configuration Management**	
CM-3	CONFIGURATION CHANGE CONTROL	CM-2
CM-4	SECURITY IMPACT ANALYSIS	CM-2
CM-5	ACCESS RESTRICTIONS FOR CHANGE	CM-2
CM-6	CONFIGURATION SETTINGS	CM-2
CM-7	LEAST FUNCTIONALITY	CM-2
CP	**Contingency Planning**	
CP-3	CONTINGENCY TRAINING	CP-2
CP-4	CONTINGENCY PLAN TESTING	CP-2
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	CP-9
IA	**Identification and Authentication**	
IA-4	IDENTIFIER MANAGEMENT	IA-2, IA-3, IA-8, IA-9, AC-3, AC-17, AC-18, AC-19
IA-5	AUTHENTICATOR MANAGEMENT	IA-2, IA-3, IA-8, IA-9, AC-3, AC-17, AC-18, AC-19
IA-6	AUTHENTICATOR FEEDBACK	IA-2, IA-3, IA-8, IA-9, AC-3, AC-17, AC-18, AC-19
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	IA-2, IA-3, IA-8, IA-9, AC-3, AC-17, AC-18, AC-19
IA-10	ADAPTIVE IDENTIFICATION AND AUTHENTICATION	IA-2, IA-3, IA-8, IA-9, AC-3, AC-17, AC-18, AC-19
IA-11	RE-AUTHENTICATION	IA-2, IA-3, IA-8, IA-9, AC-3, AC-17, AC-18, AC-19
IR	**Incident Response**	
IR-2	INCIDENT RESPONSE TRAINING	IR-4
IR-3	INCIDENT RESPONSE TESTING	IR-4
IR-5	INCIDENT MONITORING	IR-4
IR-6	INCIDENT REPORTING	IR-4

IR-7	INCIDENT RESPONSE ASSISTANCE	IR-4
IR-8	INCIDENT RESPONSE PLAN	IR-4
IR-9	INFORMATION SPILLAGE RESPONSE	IR-4
IR-10	INTEGRATED INFORMATION SECURITY ANALYSIS TEAM	IR-4
MA	**Maintenance**	
MA-2	CONTROLLED MAINTENANCE	MA-6
MA-3	MAINTENANCE TOOLS	MA-6
MA-4	NONLOCAL MAINTENANCE	MA-6
MA-5	MAINTENANCE PERSONNEL	MA-6
MP	**Media Protection**	
MP-3	MEDIA MARKING	MP-2, MP-6, MP-7
MP-4	MEDIA STORAGE	MP-2, MP-6, MP-7
MP-5	MEDIA TRANSPORT	MP-2, MP-6, MP-7
MP-8	MEDIA DOWNGRADING	MP-2, MP-6, MP-7
PE	**Physical and Environmental Protection (1. Physical access control)**	
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	PE-3, PE-4, PE-5
PE-6	MONITORING PHYSICAL ACCESS	PE-3, PE-4, PE-5
PE-8	VISITOR ACCESS RECORDS	PE-3, PE-4, PE-5
PE-10	EMERGENCY SHUTOFF	PE-9
PE-11	EMERGENCY POWER	PE-9
PE-12	EMERGENCY LIGHTING	PE-9
PE-16	DELIVERY AND REMOVAL	PE-3
PL	**Planning**	
PL-4	RULES OF BEHAVIOR	PL-2
PL-7	SECURITY CONCEPT OF OPERATIONS	PL-2
PL-8	INFORMATION SECURITY ARCHITECTURE	PL-2
PL-9	CENTRAL MANAGEMENT	PL-2
PS	**Personnel Security**	
PS-5	PERSONNEL TRANSFER	PS-2, PS-3, PS-4, PS-6
PS-8	PERSONNEL SANCTIONS	PS-7
RA	**Risk Assessment**	
RA-2	SECURITY CATEGORIZATION	PL-2
RA-3	RISK ASSESSMENT	PL-2
SA	**System and Services Acquisition (1. Development, 2. acquisition)**	
SA-2	ALLOCATION OF RESOURCES	SA-3
SA-5	INFORMATION SYSTEM DOCUMENTATION	SA-3
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	SA-3
SA-11	DEVELOPER SECURITY TESTING AND EVALUATION	SA-3
SA-13	TRUSTWORTHINESS	SA-3
SA-14	CRITICALITY ANALYSIS	SA-12
SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS	SA-3
SA-16	DEVELOPER-PROVIDED TRAINING	SA-3
SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN	SA-3
SA-19	COMPONENT AUTHENTICITY	SA-12
SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	SA-3
SA-21	DEVELOPER SCREENING	SA-3
SA-22	UNSUPPORTED SYSTEM COMPONENTS	SA-4
SC	**System and Communications Protection**	
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC-8, SC-13, SC-28, SC-40
SC-15	COLLABORATIVE COMPUTING DEVICES	
SC-16	TRANSMISSION OF SECURITY ATTRIBUTES	
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	SC-8, SC-13, SC-28, SC-40
SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	SC-8
SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	SC-8
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	SC-8
SC-24	FAIL IN KNOWN STATE	

SC-25	THIN NODES	
SC-26	HONEYPOTS	
SC-27	PLATFORM-INDEPENDENT APPLICATIONS	
SC-29	HETEROGENEITY	
SC-30	CONCEALMENT AND MISDIRECTION	
SC-32	INFORMATION SYSTEM PARTITIONING	
SC-35	HONEYCLIENTS	
SC-36	DISTRIBUTED PROCESSING AND STORAGE	
SC-37	OUT-OF-BAND CHANNELS	
SC-38	OPERATIONS SECURITY	
SC-41	PORT AND I/O DEVICE ACCESS	
SC-42	SENSOR CAPABILITY AND DATA	
SC-43	USAGE RESTRICTIONS	
SC-44	DETONATION CHAMBERS	
SI	**System and Information Integrity**	
SI-6	SECURITY FUNCTION VERIFICATION	
SI-8	SPAM PROTECTION	
SI-10	INFORMATION INPUT VALIDATION	SA-3
SI-11	ERROR HANDLING	SA-3
SI-12	INFORMATION HANDLING AND RETENTION	
SI-13	PREDICTABLE FAILURE PREVENTION	SA-3
SI-15	INFORMATION OUTPUT FILTERING	SA-3
SI-16	MEMORY PROTECTION	SA-3
SI-17	FAIL-SAFE PROCEDURES	SA-3
PM	**Program Management**	

C.5 (3) Corporate Measures

NAME	TITLE
AC	**Access Control**
AC-1	ACCESS CONTROL POLICY AND PROCEDURES
AT	**Awareness and Training**
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
AU	**Audit and Accountability**
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
CA	**Security Assessment and Authorization**
CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES
CM	**Configuration Management**
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY
CM-9	CONFIGURATION MANAGEMENT PLAN
CP	**Contingency Planning**
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES
IA	**Identification and Authentication**
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES
IR	**Incident Response**
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES
MA	**Maintenance**
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES
MP	**Media Protection**
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES
PE	**Physical and Environmental Protection (1. Physical access control)**
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
PL	**Planning**
PL-1	SECURITY PLANNING POLICY AND PROCEDURES
PS	**Personnel Security**
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES
RA	**Risk Assessment**
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES
SA	**System and Services Acquisition (1. Development, 2. acquisition)**
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
SA-8	SECURITY ENGINEERING PRINCIPLES
SC	**System and Communications Protection**
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
SC-19	VOICE OVER INTERNET PROTOCOL
SI	**System and Information Integrity**
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
PM	**Program Management**
PM-1	INFORMATION SECURITY PROGRAM PLAN
PM-2	SENIOR INFORMATION SECURITY OFFICER
PM-3	INFORMATION SECURITY RESOURCES
PM-4	PLAN OF ACTION AND MILESTONES PROCESS
PM-5	INFORMATION SYSTEM INVENTORY
PM-6	INFORMATION SECURITY MEASURES OF PERFORMANCE
PM-7	ENTERPRISE ARCHITECTURE
PM-8	CRITICAL INFRASTRUCTURE PLAN
PM-9	RISK MANAGEMENT STRATEGY
PM-10	SECURITY AUTHORIZATION PROCESS
PM-11	MISSION/BUSINESS PROCESS DEFINITION
PM-12	INSIDER THREAT PROGRAM
PM-13	INFORMATION SECURITY WORKFORCE
PM-14	TESTING, TRAINING, AND MONITORING
PM-15	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS
PM-16	THREAT AWARENESS PROGRAM

Source: NIST SP800-53r4
(last access 3/10/2019 at https://nvd.nist.gov/800-53 or https://csrc.nist.gov/publications/sp800)

Remark 1: Extended Catalogue

This annex contains the list of proposed Security Measures with basic information on the Security Dimension(s) protected.

An Extended Catalogue will be provided in an additional document and/or in the tool proposed to automate Risk Study. This Extended Catalogue will provide details on each Security Measure and will propose values for Mitigation Factors for Consequence and Likelihood of the Security Measure. These proposals are to be used to calculate the reduced likelihood and consequence of the risk and consequently the Residual RISK LEVEL (in P6 – Risk Analysis).

Remark 2: Mechanism of exception

Values for Mitigation Factors of a Security Measure are only proposals. If no value is proposed, or if the Security Risk Manager (SRM) do not agree with the proposal, he/she has the freedom to propose and use a better value based on his/her experience or preferred source.

In this case, such "exception" should simply be flagged, justified (rationale, source, …) and new value proposed keeping the spirit of the rationale for defining Mitigation Factor in remark below.

Remark 3: Rationale for defining Mitigation Factors

Estimations proposed for the different Mitigation Factors are based on the following reasoning's:

- a Mitigation Factor is a percentage (0% - 100%) of reduction on a parameter of the risk (*LIKELIHOOD* or *CONSEQUENCE*);
- a Mitigation Factor is valid for a given Security Measure against a given Threat;
- a Security Measure can have, on a given Threat, a Mitigation Factor on LIKELIHOOD and/or on CONSEQUENCE (i.e. can bring a reduction on one or both parameters);
- it is assumed that Supporting Security Measures have no effect on risks (0%); as explained above, they must be implemented together with their supported measure so that the latter can reduce the risk, but they do not reduce the risk per se;
- Mitigation Factor tends to be high for technical measures, for measures that target specific supporting asset, that are clearly specific for a threat (e.g. a backup of a data storage against any loss of availability);
- Mitigation Factor tends to be low for procedural and organisational measures, for measures that do not target specific supporting asset, that are difficult to link to any specific threat (e.g. a general awareness session);
- the relation between Mitigation Factor and Sophistication Level follows a Pareto law; at Sophistication Level 1, the mitigation is already high (proportionate to 80%), at relatively low cost; going to higher level of sophistication increases the cost exponentially while the reduction increases marginally (proportionate to 90%-95%).

List of Figures

List of Tables