NTT DATA

Executive Summary report

Ref: NTT_22-018_S4S+CYBER_REP-v1.0

As part of:

ESA Contract No. 4000135586/21/NL/AR/va

FUTURE
AT HEART

CONTROL SHEET

Title	Executive Summary report As part of: for ESA Contract No. 4000135586/21/NL/AR/va		
Author	Francisco Aguilera Leal / Patricia Rodriguez Dapena		
Reference	NTT_22-018_S4S+CYBER_REP-v1.0		
Version	1.0	***Version date***	19/Jan/2023
Reviewed by:	Patricia Rodríguez	***Revision date***	19/Jan/2023
Approved by:	Patricia Rodríguez	***Approval date***	19/Jan/2023
		Total pages	21

CHANGE CONTROL

Version	***Reason for the change***	***Responsible***	***Date***
1.0	Initial version of the document to be delivered	Francisco Aguilera Leal / Patricia Rodriguez Dapena	19/Jan/2023

INDEX

LIST OF FIGURES

LIST OF TABLES

0 Introduction

0.1 Purpose and structure of this document

The purpose and scope of this document is to present a summary of the main results of the project: the introduction of the context, a description of the programme of work and report on the activities performed and the main results achieved.

This document has the following contents:

- **Chapter 0** (this chapter) with the introduction of this document.
- **Chapter 1** introduces the scope of the project and the programme of work.
- **Chapter 2** describes the main results of the project.

0.2 Relevant Documentation

0.2.1 Applicable Documents

The following table provides the list of applicable documents and therefore they are considered as part of the baseline of the proposal.

Id.	Reference
[AD.01]	NTT Data Quality Manual
[AD.02]	TN1. Cybersecurity Development approach. Ref: EVE_21-002_CYBER+S4S_TN-v1.1
[AD.03]	TN2. Cybersecurity Model Description. Ref: NTT_22-009_S4S+CYBER_TN-v1.1
[AD.04]	PP1. Cybersecurity model presentation. Ref: NTT_22-007_S4S+CYBER_PRE-v2
[AD.05]	D1. Cybersecurity model description. Part 1 v1.1 Ref: NTT_22-004_S4S+CYBER_TN-v1.1
[AD.06]	D1. Cybersecurity model description. Part 2 v1.1 Ref: NTT_22-005_S4S+CYBER_TN-v1.1
[AD.07]	PP2. Training slides for assessors Ref: NTT_22-011_S4S+CYBER_PRE-v2
[AD.08]	PP3. Training slides for organizations. Ref: NTT_22-012_S4S+CYBER_PRE-v1.0
[AD.09]	Brochure + Video Ref: NTT_22-013_S4S+CYBER_PRE-v1.0

Table 1 List of applicable documents

0.2.2 Reference Documents

The following table provides the list of referenced documents and therefore not considered as part of the baseline of the proposal but used to support its content.

Id.	Reference
[RD.01]	ECSS-Q-ST-80C Rev.1, Space product assurance – Software productassurance
[RD.02]	ECSS-Q-HB-80-02 Part 1A, Space product assurance – Software processassessment and improvement – Part 1: Framework
[RD.03]	ECSS-Q-HB-80-02 Part 2A, Space product assurance – Software processassessment and improvement – Part 2: Assessor instrument
[RD.04]	ECSS-E-ST-10C Rev.1, Space engineering – System engineering generalrequirements
[RD.05]	ECSS-E-ST-40C, Space engineering – Software.
[RD.06]	ECSS-E-HB-40-01A, Space engineering – Agile software developmenthandbook
[RD.07]	ISO/IEC 33001:2015, Information technology – Process assessment –Concepts and terminology
[RD.08]	ISO/IEC 33004:2015, Information technology – Process assessment –Requirements for process reference, process assessment and maturity models
[RD.09]	ISO/IEC 33002:2015, Information technology -- Process assessment -- Requirements for performing process assessment

[RD.10]	ISO/IEC 33020:2019, Information technology – Process assessment – Process measurement framework for assessment of process capability
[RD.11]	ISO/IEC TS 33061:2021. Information technology — Process assessment — Process assessment model for software life cycle processes
[RD.12]	ISO/IEC 12207:2017 ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes
[RD.13]	ISO/IEC 15504-5:2006 Information technology — Process assessment — Part 5: An exemplar software life cycle process assessment model
[RD.14]	ISO/IEC 27036-1:2014. Information technology — Security techniques — Information security for supplier relationships. Parts.

Table 2 List of reference documents

0.3 Acronyms

Acr	Definition
ARCS	Assessor Registration and Certification Scheme
C2M2	Cybersecurity Capability Maturity Model
CMMC	Cybersecurity Maturity Model Certification
CMMI	Capability Maturity Model Integration
cPPP	contractual Public Private-Partnership
DoD	Department of Defence
E/E	Electrical and Electronic
ECSS	European Cooperation for Space Standardization
ENISA	European Union Agency for Cybersecurity
IEC	International Electrotechnical Commission
INTACS	International Assessor Certification Scheme
ISO	International Organization for Standardization
ISVV	Independent Software Verification Validation
ITU	International Telecommunication Union
MM	Maturity Model
NIST	United States National Institute of Standards and Technology
PAM	Process Assessment Model
PRM	Process Reference Model
S4S	Security for Safety
SAE	Society of Automobile Engineers
SOW	Statement of Work
UN ECE	United Nations Economic Commission for Europe
VDA	Verband der Automobilindustrie

1 Scope of the project

1.1 Introduction

Like any other increasingly digitized critical system, satellites and other space-based assets are vulnerable to cyberattacks. These cyber vulnerabilities pose serious risks not just for flight-based assets themselves but also for ground-based critical segments, therefore need to be contained.

For the European space domain, the software is requiring ‘possessing’ different characteristics such as safety and dependability, among others and increasingly now, in particular as the subject of this project, ‘containing’ (cyber)security aspects.

This project was NOT intended to define a standard for products’ cybersecurity but to define the cybersecurity development processes’ models through which the product characteristic is to be implemented. It is a process-based standard to be used to define and assess processes, with which the end product should meet the desired results for the products in the in the space domain.

The cybersecurity development processes and their assessment model and maturity model were to be integrated with current existing ECSS standards as well as the S4S process assessment models contained in ECSS-Q-80-HB-02 Parts 1/2 (in [RD.02] and [RD.03]).

ECSS-Q-80-HB-02 Parts 1/2 (S4S) provides processes both the Process Reference Model (PRM) as well as the Process Assessment Model (PAM) together with assessor guides for performing assessments to software suppliers in the European space domain. This so called S4S models focus on software life cycle processes, copying the ISO/IEC 15504-5:2006 [RD.13], adding to it notes, processes (4 processes), base practices and work products needed and explicitly required by ECSS not covered in the ISO more generic one. Figure below presents those four processes and also examples of the added notes, base practices and work products.

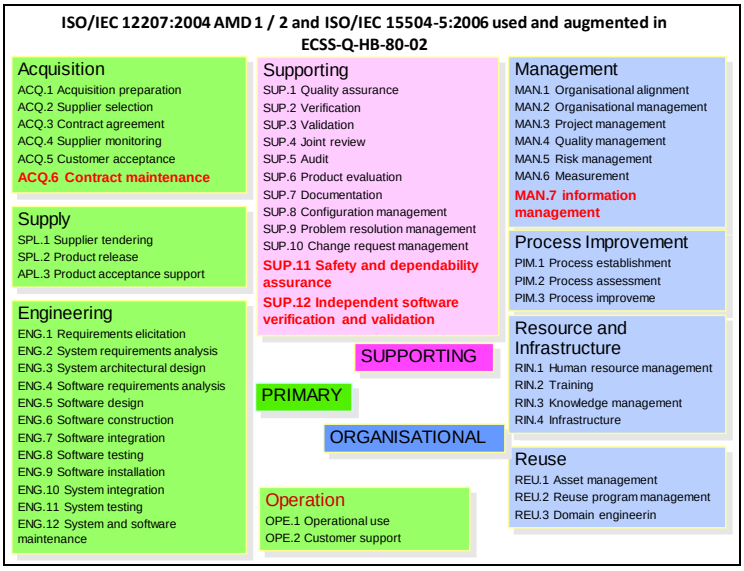
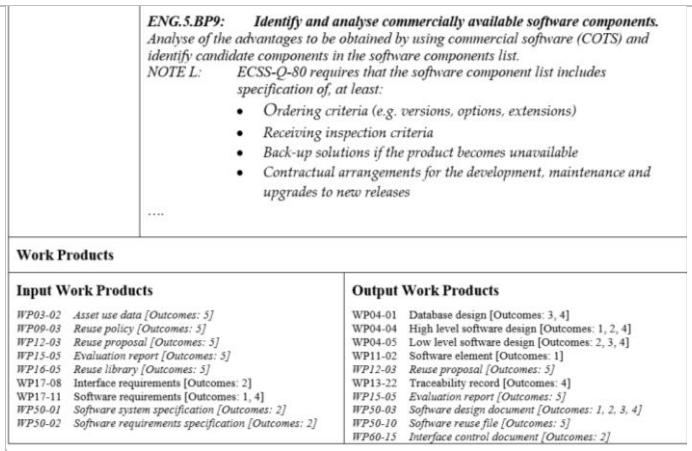


Figure 1 S4S processes (the added ones are in bold / pink)



ENG.5.BP9: ***Identify and analyse commercially available software components.***
Analyse of the advantages to be obtained by using commercial software (COTS) and identify candidate components in the software components list.
NOTE L: *ECSS-Q-80 requires that the software component list includes specification of, at least:*

- *Ordering criteria (e.g. versions, options, extensions)*
- *Receiving inspection criteria*
- *Back-up solutions if the product becomes unavailable*
- *Contractual arrangements for the development, maintenance and upgrades to new releases*

....

Work Products

Input Work Products		Output Work Products	
WP03-02	*Asset use data [Outcomes: 5]*	WP04-01	Database design [Outcomes: 3, 4]
WP09-03	*Reuse policy [Outcomes: 5]*	WP04-04	High level software design [Outcomes: 1, 2, 4]
WP12-03	*Reuse proposal [Outcomes: 5]*	WP04-05	Low level software design [Outcomes: 2, 3, 4]
WP15-05	*Evaluation report [Outcomes: 5]*	WP11-02	Software element [Outcomes: 1]
WP16-05	*Reuse library [Outcomes: 5]*	*WP12-03*	*Reuse proposal [Outcomes: 5]*
WP17-08	Interface requirements [Outcomes: 2]	WP13-22	Traceability record [Outcomes: 4]
WP17-11	Software requirements [Outcomes: 1, 4]	*WP15-05*	*Evaluation report [Outcomes: 5]*
WP50-01	*Software system specification [Outcomes: 2]*	*WP50-03*	*Software design document [Outcomes: 1, 2, 3, 4]*
WP50-02	*Software requirements specification [Outcomes: 2]*	*WP50-10*	*Software reuse file [Outcomes: 5]*
		WP60-15	*Interface control document [Outcomes: 2]*

Figure 2 Example of ISO/IEC 15504-5 with added base practices, notes and work products

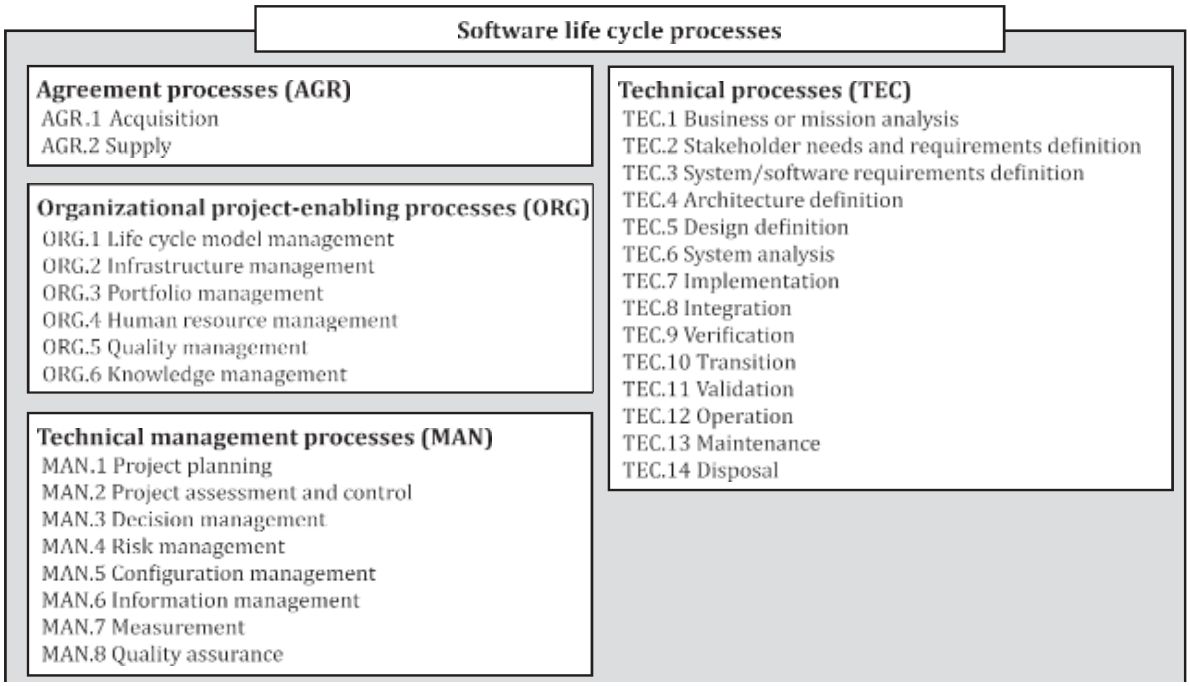


Figure 3 ISO/IEC 33061 processes [RD.11]

It is important to note that during the performance of the project, the S4S model was under revision and would be updated to the latest version of ISO/IEC 12207:2017 processes and ISO/IEC 33061:2021 process assessment model:

None of above models contain cybersecurity processes per se, but the new ISO/IEC 33061 [RD.03] (based on the ISO/IEC 12207:2017 version [RD.12]) contains references to Security within the processes, the assessment model indicators, etc. as recognised to be an increasing concern in systems and software engineering. It refers to ISO/IEC 27036, Security techniques - Information security for supplier relationships [RD.14], for requirements and guidance for suppliers and acquirers on how to secure information in supplier relationships. Specific aspects of information security supplier relationships are addressed in ISO/IEC 27036-3:2013 and ISO/IEC 27036-4 [RD.14].

In further paragraphs and sections the S4S models and scope are introduced while analysing the project requirements and presenting this proposal.

This project was requiring identifying the cybersecurity process reference model, Process Assessment Model and Maturity Model and process improvement guidelines, together with presentation materials that can be employed for defining, controlling, and improving software life cycle processes within an organization or a project concerning the cybersecurity aspects in space domain products.

Above objective was implemented in the following activities as required in the SOW:

1. Select and define the approach to be used for the cybersecurity process and models appropriate for the European space industry to follow for the development of the process assessment and improvement model.
2. Development of a model for process assessment and improvement for cybersecurity in the European space industry.
3. Documentation of the cybersecurity model in a handbook, based on the results of above goal 1, the cybersecurity model(s) documentation shall include the Process Assessment Model, the Process Reference Model and a guide for Assessors, and all if possible following the style of ECSS handbooks.
4. Development of training material for the cybersecurity model: for which the training material shall consist of two sets of slides: one for assessors and one for organisations planning an assessment.

Each of the above activities were going to be analysed in the following sections with introductory aspects needed for each of them.

1.2 Objectives

The project had three main objectives:

- Development of a model for process assessment and improvement for cybersecurity in the European space industry.
  1. The model to be according to one of the approaches described in section 2.1 of the SOW.
  2. The model to focus on the security of software development processes (as opposed to the security of work products) [Criterion 1].
  3. The model to be appropriate for suppliers of space segment components as well as to suppliers of ground segment components and its infrastructure [Criterion 2].
  4. The model to take into account – where applicable – the specific nature of space industry projects. This includes, but is not limited to, aspects like:

- the international context in which space systems are developed and operated, and – as a consequence – the variety of regulatory requirements that may apply [Criterion 3];
- the importance of safety and dependability assurance and the potential conflicts that may arise between safety and security requirements [Criterion 4];
- safety- and mission-criticality (including manned missions) [Criterion 5];
- the specific setup of industry consortia [Criterion 6];
- the ECSS standards and their tailoring mechanisms [Criterion 7];
- the use of independent software verification and validation (ISVV) [Criterion 8];
- the long lifetimes of many of the projects [Criterion 9];
- the specific development phases and lifecycles of space projects (see [RD4] [RD5] [RD6]) [Criterion 10];
- the fact that space systems can often not be updated, modified or maintained in-flight [Criterion 11]; and
- the fact that communication with space systems is not always possible in (near-)real-time [Criterion 12].

- Documentation of the cybersecurity model in a handbook, to include the Process Assessment Model, the Process Reference Model and a guide for Assessors. If possible, the documentation to follow the style of ECSS handbooks.
- Development of training material for the cybersecurity model, consisting of two sets of slides: one for assessors and one for organisations planning an assessment.

No TRL requirements apply to this Statement of Work as there is no equipment, component, neither flight software nor flight hardware product as a result.

2 Main results of the project

2.1 Cybersecurity process models

The main result of this project is the cybersecurity model, including all its components and models.

This documentation was now requested follow the style of ECSS handbooks, and also being:

- complete, structured and understandable.
- formal in the sense that all external sources are correctly referenced.
- making a clear distinction between normative and informative aspects of the model.

The results of this task consisted in two documents:

- D1. Cybersecurity model description. Part 1 v1.1 [AD.05]: This handbook (Part 1) provides the instruments and information to determine the level of process performance and capability, to improve the software processes identifying the changes or additions that should be done, and to ensure that all ECSS requirements are met for a given project.
- D1. Cybersecurity model description. Part 2 v1.1 [AD.06]: This handbook (Part 2) provides assessors with a number of instruments needed to perform software process capability assessments using the assessment method described in Part 1. It also provides instruments that help assessors to carry out their activities when performing assessments and supporting the implementation of software process improvement initiatives using the method for process improvement described in Part 1. The instruments provided are:

- The Process Assessment Model (PAM) required to perform ECSS-Q-HB-80-02 assessments including process descriptions and process attribute indicators
- Conformance statement to the requirements in ISO/IEC 33004
- A definition of the Process Reference Model (PRM) on which the ECSS-Q-HB-80-02 PAM is based upon
- Detailed traces from base practices in the ECSS-Q-HB-80-02 PAM to ECSS standards clauses and from ECSS-Q-HB-80-02 process outputs to ECSS expected outputs

2.1.1 D1. Cybersecurity model description. Part 1 [AD.05]

2.1.1.1 Introduction of the models

Part 1 of the handbook presents an overall introduction of the models detailed in Part 2. The bidimensional assessment model, composed by the process dimension and the capability dimension:

a) the process dimension, which is characterized by process purposes which are the essential measurable objectives of a process;

b) the process capability dimension, which is characterized by a series of process attributes, applicable to any process, which represent measurable characteristics of a process.

Process description component	ECSS term
Process ID + Process name	Requirements, process, activity or task name
Process purpose	Requirement, process, activity or task definition
Process outcome	Requirements, process or activity definition
Process notes	

Table 3 Process description components

In comparison with the process dimension of the exemplar process assessment model in ISO/33061 (from ISO/IEC 12207:2017), the S4S process dimension was augmented with space specific processes, including new base practices and outputs. Every process of the exemplar software process assessment model in ISO/IEC 33061 is embedded in S4S, as they were either matched with the expected outputs of ECSS requirements or, where no match was found, remain in S4S as-is. New process outputs and output descriptions were created to represent specific ECSS outputs not covered by the ISO/IEC 33061 exemplar model. The new processes and indicators properly incorporate space software requirements into the S4S process assessment model.

Finally, the process dimension of the S4S PAM has been further extended with cybersecurity related processes based on other cybersecurity standards and refined for the space context.

The following table lists the processes of the S4S process dimension and shows their classification in different process groups. A detailed description of the process is included in Part 2 of this guideline.

Group	Processes
Agreement processes (AGR)	AGR.1 Acquisition AGR.2 Supply AGR.3(**) Cybersecurity Supplier Request and Selection

Organizational project-enabling processes (ORG)	ORG.1 Life cycle model management ORG.2 Infrastructure management ORG.3 Portfolio management ORG.4 Human resource management ORG.5 Quality management ORG.6 Knowledge management
Technical management processes (MAN)	MAN.1 Project planning MAN.2 Project assessment and control MAN.3 Decision management MAN.4 Risk management MAN.5 Configuration management MAN.6 Information management MAN.7 Measurement MAN.8 Quality assurance MAN.9(*) Safety and dependability MAN.10(*) Independent Software Verification and Validation MAN.11(**) Cybersecurity Risk Management
Technical processes (TEC)	TEC.1 Business or mission analysis TEC.2 Stakeholder needs and requirements definition TEC.3 System/ software requirements definition TEC.4 Architecture definition TEC.5 Design definition TEC.6 System analysis TEC.7 Implementation TEC.8 Integration TEC.9 Verification TEC.10 Transition TEC.11 Validation TEC.12 Operation TEC.13 Maintenance TEC.14 Disposal
Security engineering processes (SEC)	SEC.1(**) Cybersecurity Requirements Elicitation SEC.2(**) Cybersecurity Implementation SEC.3(**) Risk Treatment Verification SEC.4(**) Risk Treatment Validation SEC.5(**) Cybersecurity in Operations
(*) : processes added in ECSS-Q-HB-80-02 handbook w.r.t the ones in ISO/IEC 33061 (**): processes added in this technical note w.r.t the ones in ISO/IEC 33061 from ASPICE SEC processes (also marked up in blue)	

Table 4 ECSS-Q-HB-80-02 set of processes including processes for cybersecurity

The capability dimension defines a measurement scale for the capability of any process. The capability dimension scale adopted in this handbook is the one from ISO/IEC 33061. There are no space specific modifications, therefore, six point ordinal scale is defined, representing an increasing capability of the performed process. At the bottom end of the scale, process performance does not achieve the purpose of the process, while at the top end of the scale, process performance is capable to meet relevant process and improvement goals that are

explicitly derived from the organization’s business goals. The scale therefore derives a well-defined route for improvement for each individual process.

The process attributes (PA) are following the latest ISO/IEC 33020 standard, defining the following PAs:

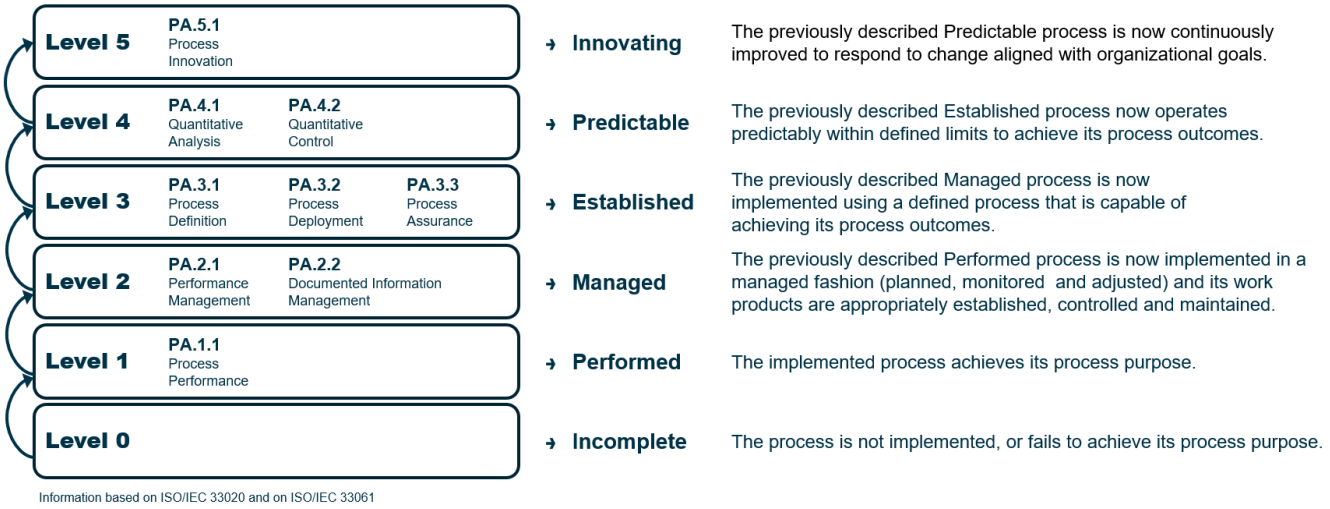


Figure 4 Process capability dimension/Measurement framework [RD.10]

2.1.1.2 Process assessment process guidelines

An assessment is divided into the following tasks following the diagram of the assessment process provided in the next Figure:

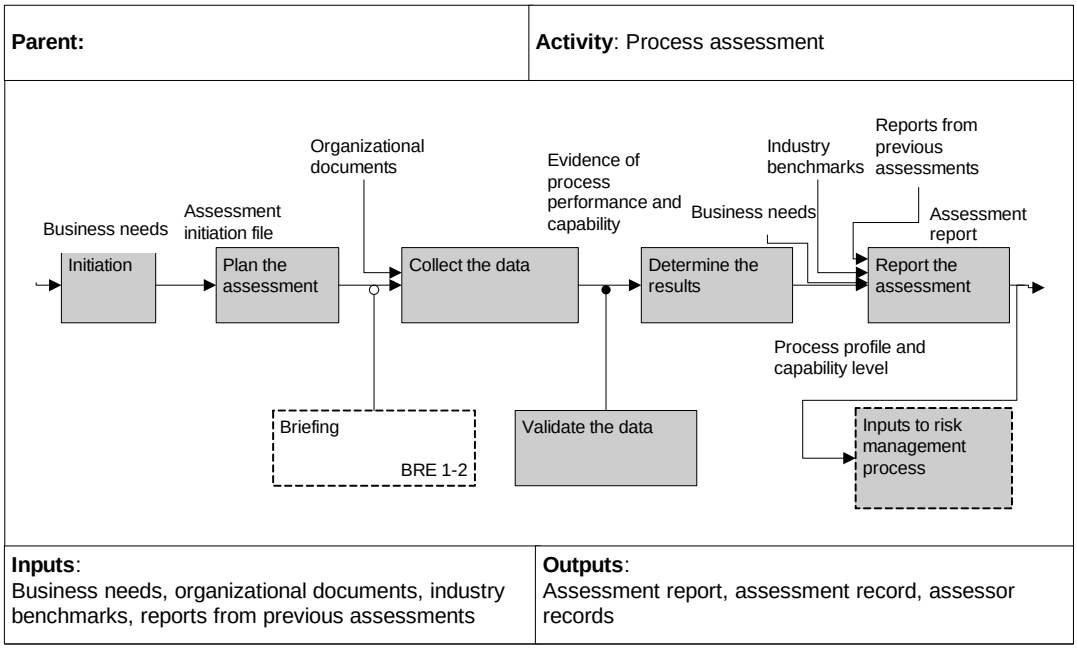


Figure 5 The assessment process definition

Part 1 of the guidelines further details each of above process assessment activities providing a detailed breakdown of each activity into tasks, including the main results of each task as well as the roles involved in their performance. S4S assessment activities, roles or work products are marked with symbols found at the end of lines of text, intended to trace to the source from which the different phrases/requirements are from and to be used for the conformance statements:

❶: The preceding phrases/requirements are justified by requirements of the normative parts of ISO/IEC 33002 [RD.09]

❷: The preceding phrases/requirements are justified by information from guidance parts of ISO/IEC 33010 (still draft).

❸: The preceding phrases/requirements are justified by best industry practice

❹: The preceding phrases/requirements are justified by requirements from ECSS Standards

Each assessment process activity is presented following the same layout for each of them, including:

- Objective of each activity,
- Detailed steps and
- Input and output work products.

Each detailed step includes in turn:

- its objective,
- the expected outputs and
- the roles responsible for their performance

All detailed steps defined are uniquely identified to correspond to the different boxes defined in the diagrams.

The participant parties for the different activities and detailed tasks are defined using the following acronyms:

AP	assessment participants
AS	assessment sponsor
AT	assessment team
ATL	assessment team leader
LA	lead assessor
LAC	local assessment coordinator
OU	organizational unit

Detailed information about these roles is also provided in the guideline. The responsible party of the activities is put between () in the diagrams of each detailed task.

2.1.1.3 Improvement process guidelines

Part 1 of the handbook contains a detailed process definition for any process improvement project to be performed.

The steps or activities of the process improvement are based on the ISO/OEC 33014 guideline, highlighting only the perspective of process improvement only containing activities at tactical and operational levels.

Each process major step and activities is represented following the same notation as for the process assessment guidelines, including all responsibles, activities, input and outputs of all activities.

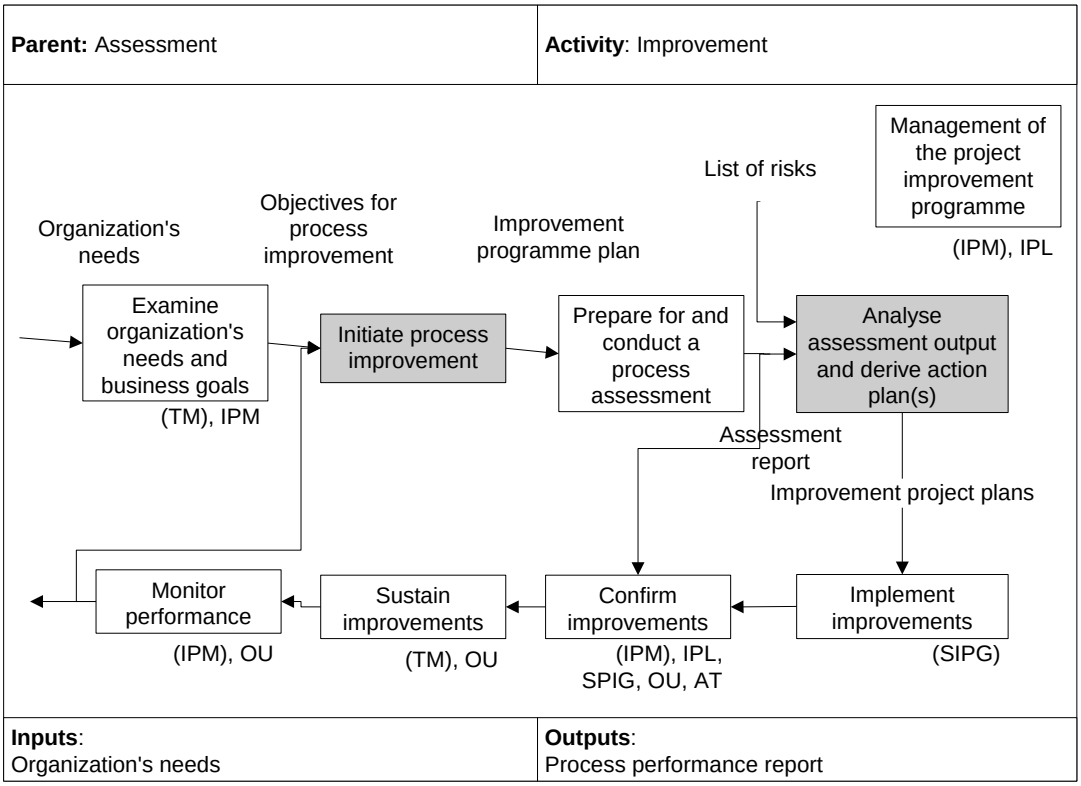


Figure 6 Improvement activities

The guideline further details each of above improvement activities providing a detailed breakdown of each activity into tasks, including the main results of each task as well as the roles involved in their performance.

It is important to have clear definition of roles and responsibilities in an improvement plan. Seven main roles are identified in the guidelines. These roles are mainly equivalent to the roles from ISO/IEC 33014. The roles practitioner and project manager from the standard have been merged into a single role in this handbook. Additionally, the process improvement team has been separated into two roles: the improvement project leader and the software process improvement group.

- Top management (TM)
- Improvement programme manager (IPM)
- Improvement project leader (IPL)
- Software process improvement group (SPIG) members
- Process owners (PO)
- (Staff of the) Organizational unit (OU)
- Assessment Team (AT)

Different roles can be involved in a given step. Some can be responsible for it, others contribute or participate always and others participate or not depending on the circumstances. The responsible role is represented in each step between (). The roles whose participation is optional are presented in italics.

2.1.1.4 Target profiles

The proposed target profile in table below contains a set of processes identified as highly significant and forming the S4S minimum scope, considered as the minimum to be selected for an

assessment. In case of software of criticality levels A or B, MAN.9 and MAN.10 are to be included. Some processes included in the target profile are to be in scope of an assessment only when performed by the organisation, such is the case for the SEC group of processes.

Process ID	Process Title	Capability Level			
		A	B	C	D
MAN.1	Project planning	3	3	2	2
MAN.2	Project assessment and control	3	3	2	2
MAN.5	Configuration Management	3	3	2	2
MAN.8	Quality assurance	3	3	2	2
MAN.9*	Safety and dependability assurance	3	3	0	0
MAN.10*	Independent software verification and validation	3	3	0	0
TEC.3	System/Software requirements definition	3	3	2	2
TEC.4	Architecture definition	3	3	2	2
TEC.5	Design definition	3	3	2	2
TEC.7	Implementation	3	3	2	2
TEC.8	Integration	3	3	2	2
TEC.11	Validation	3	3	2	2
SEC.1	Cybersecurity requirements elicitation	3	3	2	2
SEC.2	Cybersecurity implementation	3	3	2	2
SEC.3	Risk treatment verification	3	3	2	2
SEC.4	Risk treatment validation	3	3	2	2
(*)To be in scope as applicable					

Table 5 Proposed target profile

2.1.1.5 Recommendations for the content of SW process assessment outputs

This handbook Part 1 refers to a number of documents that are outputs of the software assessment process and improvement methods. The specific structure of most of these documents is left to the assessors and organizations involved in the different activities, however contents of some documents have a particular relevance in confirming the correct application of the methods described or in confirming compliance with requirements in ECSS-Q-ST-80 rev.1 or ISO/IEC 330xx family standards.

Annex B of Part 1 of the handbook provides the proposed contents of the following process assessment outputs:

- Assessment plan
- Assessment report (including the assessment record)

2.1.2 D1. Cybersecurity model description. Part 2 [AD.06]

Part 2 of the handbook incorporates cybersecurity-related processes into the scope of the ECSS-Q-HB-80-02A assessments. It defines additional indicators specific for these cybersecurity processes. As a result::

- The Process Reference Model (PRM) in chapter 4 contains new cybersecurity related processes.

- The Process Assessment Model (PAM) in chapter 5 includes process descriptions and process attribute indicators for the new cyber security processes.

This Part 2 has been defined having as reference the cybersecurity adaptations of the. Automotive SPICE processes being a common framework for the assessment of suppliers in the Automotive Industry. It defines a PAM used to perform conformant assessments of the software process capability of automotive suppliers in accordance with the requirements of ISO/IEC 33002. It has its own PRM, which was developed based on ISO/IEC 12207 and now adding cybersecurity processes based on different regulations and standards such as: ISO UN ECE 155, ISO 21343).

2.1.2.1 The Process Reference Model

The Process Reference Model is suitable for use in process assessment performed in accordance with ISO/IEC 33002, Information technology — Process assessment — Part 2: Performing an assessment. A statement of conformance with the requirements from ISO/IEC 33004 is included in Annex B of this Part 2 document.

Each process of this document is described in terms of the following attributes:

- The title conveys the scope of the process as a whole
- The purpose describes the goals of performing the process
- The outcomes express the observable results expected from the successful performance of the process

Table 4 ECSS-Q-HB-80-02 set of processes including processes for cybersecurityabove presented the new process set. Part 2 details the list of processes of the new S4S model including the cybersecurity ones.

In order to facilitate the identification of the sources of the different processes some components of the process descriptions have been coloured differently. Components of the process descriptions inherited from ISO/IEC 12207 [ISOIEC 12207:2017] are shown in normal text. Components inherited from the previous ECSS-Q-HB-80-02 standard for the space domain are shown in *italics*. Cybersecurity-related additions originally from Automotive SPICE are shown in colour **green** and further additions specific for space are shown in ***blue and italics***.

The following paragraphs present a couple of samples of these processes detailed definition:

4.8.5 → Risk·treatment·validation·process·(SEC.4)¶

4.8.5.1 → Purpose¶

The·purpose·of·the·Risk·treatment·validation·process·is·to·confirm·that·the·integrated·system·achieves·the·associated·cybersecurity·goals.¶

4.8.5.2 → Outcomes¶

As·a·result·of·the·successful·implementation·of·the·Risk·treatment·validation·process:¶
a)→A·risk·treatment·validation·strategy·is·developed,·implemented·and·agreed·upon·with·relevant·stakeholders·and·maintained·suitably·to·provide·evidence·that·the·implementation·achieves·the·associated·cybersecurity·goals.¶
b)→The·implemented·design·and·integrated·components·are·validated·according·to·the·defined·risk·treatment·validation·strategy.¶
c)→Validation·activities·are·documented·and·the·results·recorded.¶
d)→Traceability·between·the·cybersecurity·goals,·risk·treatment·validation·specification·and·validation·results·is·established.¶
e)→Consistency·between·the·cybersecurity·goals·and·the·risk·treatment·validation·specification·is·established.¶
f)→Results·of·the·validation·are·summarized·and·communicated·to·all·affected·parties.¶

4.8.6 → Cybersecurity in operations process (SEC.5)

4.8.6.1 → Purpose

The purpose of the cybersecurity in operations process is to ensure that the system is used in a secure manner after development. This includes the delivery and installation of software, the operation, its maintenance and the disposal of software components.
This process establishes additional cybersecurity requirements and assigns responsibilities for the operational phase of the system, and monitors the services and operator-system performance with regards to security. It identifies anomalies in relation to cybersecurity requirements and constraints.

4.8.6.2 → Outcomes

As a result of the successful implementation of the cybersecurity operation process:
a) Mechanisms for secure software delivery, installation and configuration are established and documented.
b) Security awareness and training is spread among users, operators and system owners.
c) Operational cybersecurity tests are defined and performed.
d) Monitoring of cybersecurity of the system is performed and security incidents are discovered, reported and managed.
e) Security considerations are considered in modification and disposal of software.

Figure 7 Samples of processes's definition in Part 2

2.1.2.2 The Process Assessment Model

The process attributes in the capability dimension (based on ISO/IEC 33020:2019, presented in above Figure 4 have a set of process capability indicators that provide an indication of the extent of achievement of the process attribute in the instantiated process. These indicators concern significant activities, resources or results associated with the achievement of the process attribute purpose by a process. These process capability indicators are the generic practices (GP).

As additional indicators for supporting the assessment of a process at Level 1, each process in the process dimension has a set of process performance indicators which is used to measure the degree of achievement of the process performance attribute for the process assessed: The process performance indicators are used to measure the degree of achievement of the process performance attribute (PA.1.1) for the process assessed.

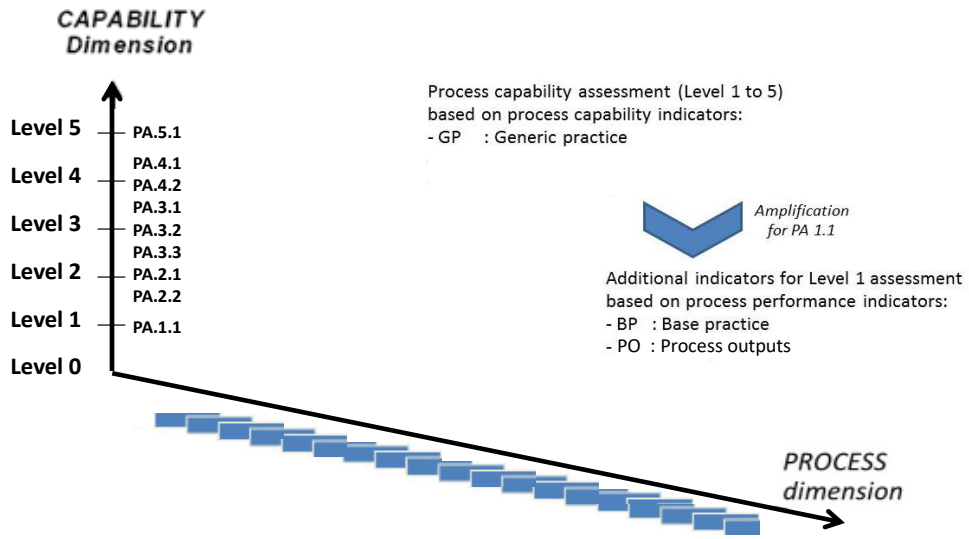


Figure 8 Assessment indicators [ISO 33061]

These types of indicators help to establish objective evidence of the extent of achievement of the specified process attribute.

There are two types of process performance indicators; base practice (BP) indicators and process output (PO) indicators. Process performance indicators relate to individual processes defined in the process dimension of the process assessment model and are chosen to explicitly address the achievement of the defined process purpose.

Evidence of performance of the base practices and the presence of process outputs with their expected process output characteristics provide objective evidence of the achievement of the purpose of the process.

A base practice is an activity that addresses the purpose of a particular process. Consistently performing the base practices associated with a process will help the consistent achievement of its purpose. A coherent set of base practices is associated with each process in the process dimension. The base practices are described at an abstract level, identifying “what” should be done without specifying “how”. Implementing the base practices of a process should achieve the basic outcomes that reflect the process purpose. Base practices represent only the first step in building process capability, but the base practices represent the unique, functional activities of the process, even if that performance is not systematic. The performance of a process produces process outputs that are identifiable and usable in achieving the purpose of the process. In this assessment model, each process output has a defined set of example process output characteristics that may be used when reviewing the process output to assess the effective performance of a process. Process output characteristics may be used to identify the corresponding process outputs produced/used by the assessed organization.

Chapter 5 of Part 2 contains a complete description of the processes, including the base practices and the associated process outputs. Each base practice has its own identifier.

The following table (based on ISO/IEC 33061 and the ASPICE SEC processes and PAM) presents a sample of one of these processes, following the same protocol as for the PRM: Components inherited from the previous ECSS-Q-HB-80-02 standard for the space domain are shown in *italics*. Cybersecurity-related additions originally from Automotive SPICE are shown in colour **green** and further additions specific for space are shown in ***blue and italics***:

Process ID	**SEC.2**
Process name	**Cybersecurity implementation process**
Process purpose	The purpose of the cybersecurity implementation process is to allocate the cybersecurity requirements to the elements of the system and software and ensure they are implemented.
Process outcomes	As a result of the successful implementation of the cybersecurity implementation process: The architectural design is refined. Cybersecurity requirements are allocated to elements of the architectural design. Appropriate cybersecurity controls are selected. Vulnerabilities are analysed. The detailed design is refined. Software units are developed. Consistency and *traceability* are established between architectural design and detailed design. The cybersecurity risk treatment implementation is agreed upon and communicated to all affected parties.
Base practices	**SEC.2.BP1: Refine the details of the architectural design.** [Outcome: a] 1) The architectural design is refined based on cybersecurity goals and cybersecurity requirements. NOTE 1: Refinement could be on system or software level architecture. NOTE 2: Refinement here means to add, adapt or rework elements of the architecture. *NOTE I: ESSB-ST-E-008 requires a review of security specific design elements in the Critical Design Review.* **SEC.2.BP2: Allocate cybersecurity requirements.** [Outcome: b] 1) Allocate the cybersecurity requirements to one or more elements of the architectural

	design. NOTE 3: Cybersecurity requirements could be on system and software level. *NOTE II: ESSB-ST-E-008 requires updates of the cybersecurity risk assessment based on the outcome of the transformation of the software cybersecurity requirements into elements of the software architectural and detailed design.* **SEC.2.BP3: Select cybersecurity controls.** [Outcome: c] 1) Select appropriate cybersecurity controls to achieve or support the cybersecurity requirements. NOTE 4: Typically, cybersecurity controls are technical solutions to avoid, detect, counteract or minimize cybersecurity risks. *NOTE III: Cybersecurity control might be also imposed on the development and integrating environment. ESS-ST-E-008 requires such requirements to be defined by the customer based on the security sensitivity of the system* **SEC.2.BP4: Refine interfaces.** [Outcome: a] 1) Refine and describe cybersecurity related interfaces between the elements of the architectural design and operating environment. **SEC.2.BP5: Analyse architectural design.** [Outcome: d] 1) Analyse the architectural design to identify and analyse vulnerabilities. **SEC.2.BP6: Refine the details of the detailed design.** [Outcome: e] 1) The detailed design is refined based on architectural design. NOTE 5: Refinement here means to add, adapt or rework components of the detailed design. **SEC.2.BP7: Develop software units.** [Outcome: f] 1) Implement the software using appropriate modeling or programming languages. NOTE 6: Criteria for appropriate modelling and programming languages for cybersecurity can include the use of language subsets, enforcement of strong typing and/or the use of defensive implementation techniques. NOTE 7: Example to cover the defined criteria could be the use of a coding guideline or an appropriate development environment. **SEC.2.BP8: Establish *traceability*.** [Outcome: b, g] 1) Establish complete traceability between the refined architectural design and the detailed design. **SEC.2.BP9: Ensure consistency.** [Outcome: g] 1) Ensure consistency between the refined architectural design and the detailed design. **SEC.2.BP10: Communicate agreed results of cybersecurity implementation** [Outcome: h] 1) Communicate the agreed results of the cybersecurity implementation to all affected parties including stakeholders from post-development phases. NOTE 8: The communicated contents may include both results of the cybersecurity implementation and vulnerabilities identified within the architectural design analysis.
Process outputs	Software architectural design [Outcome: a] Software detailed design [Outcome: e] System architectural design [Outcome: a] Software unit [Outcome: f] Communication record [Outcome: h] Review record [Outcome: g] Traceability *mapping* [Outcome: b, g] Vulnerability analysis report [Outcome: d] Cybersecurity controls [Outcome: c]

Chapter 6 of Part 2 contains a complete description of the process attributes, including the generic practices, copying the materials from ISO/IEC 33020:2019 for each process attribute and their indicators respectively.

Annex A of Part 2 contains a complete list of specific and generic process output. An assessor would refer to the specific process outputs when performing an assessment. The following table provides a sample of these detailed definitions:

…			
Critical performance measurement needs	Identification of information needs of the decision makers with respect to system of interest (including software as a system) expectations. [Adapted from INCOSE SE Handbook 2015]	specification	TEC.2, TEC.3, TEC.4, TEC.5
Cybersecurity goals	Concept-level cybersecurity requirements associated with one or more threat scenarios. [ISO/SAE 21434]	description	SEC.1
Cybersecurity controls	Technical solutions to prevent, detect, or mitigate cybersecurity risks Associated to one or more cybersecurity requirements [Adapted from ISO/SAE 21434]	description	SEC.2
…			

Table 6 Sample of outputs definitions

Annex B of Part 2 presents B.1 a self-statement of conformity of the process reference model and the process assessment model versus the requirements of ISO/IEC 33004 respectively for both models.

Annex C of Part 2 also presents the traces to the ECSS standards as applicable.

2.2 Training materials – WP4000

Training materials of the models defined is the other main result of this project. The following sets of materials were produced:

1) PowerPoint slides set 1 for introducing and summarising the models produced
2) Power Point slides set 2 for familiarising assessors with the new model. The intention of these slides is not to formally train assessors. Rather, the aim is to acquaint assessors who are already certified for S4S with the new model.
3) PowerPoint slides set 3 for introducing organisations to be assessed to the cybersecurity model. This set of slides shall take into account that a cybersecurity assessment may be performed together with an S4S process capability assessment, or by itself. The set of slides shall not focus on capability assessments, but shall take into account that its target audience doesn't necessarily have any previous experience with SPICE or CMMI. It is to focus on all aspects of the cybersecurity model relevant for the organisation, leaving out the more technical details relevant to the assessors.
4) Additional training material was produced for dissemination of the models:
    1. A brochure
    2. A video.

2.3 List of deliverables from the project

Table below summarizes the main results of this project:

Reference	Title	Introduction
EVE_21-002_CYBER+S4S_TN-v1.1	TN1. Cybersecurity Development approach	Analysis of different existing approaches for cybersecurity processes when engineering and operating security-critical systems
NTT_22-009_S4S+CYBER_TN-v1.1	TN2. Cybersecurity Model Description	Aims to extend the coverage of the process assessments in the space industry with cyber-security aspects. It enhances ECSS-Q-HB-80-02A, which is separated in two documents: the description and guidance of assessment framework (Part 1) and the instruments used for the assessment (Part 2).

NTT_22-007_S4S+CYBER_PRE-v2	PP1. Cybersecurity model presentation	Aims to present the Cybersecurity Model, and how the coverage of the process assessments in the space industry with cyber-security aspects enhances ECSS-Q-HB-80-02A.
NTT_22-004_S4S+CYBER_TN-v1.1	D1. Cybersecurity model description. Part 1 v1.1	This handbook (Part 1) provides the instruments and information to determine the level of process performance and capability, to improve the software processes identifying the changes or additions that should be done, and to ensure that all ECSS requirements are met for a given project.
NTT_22-005_S4S+CYBER_TN-v1.1	D1. Cybersecurity model description. Part 2 v1.1	This handbook (Part 2) provides assessors with a number of instruments needed to perform software process capability assessments using the assessment method described in Part 1. It also provides instruments that help assessors to carry out their activities when performing assessments and supporting the implementation of software process improvement initiatives using the method for process improvement described in Part 1. The instruments provided are: • The Process Assessment Model (PAM) required to perform ECSS-Q-HB-80-02 assessments including process descriptions and process attribute indicators • Conformance statement to the requirements in ISO/IEC 33004 • A definition of the Process Reference Model (PRM) on which the ECSS-Q-HB-80-02 PAM is based upon • Detailed traces from base practices in the ECSS-Q-HB-80-02 PAM to ECSS standards clauses and from ECSS-Q-HB-80-02 process outputs to ECSS expected outputs
NTT_22-011_S4S+CYBER_PRE-v2	PP2. Training slides for assessors	PP2. Training slides for assessors
NTT_22-012_S4S+CYBER_PRE-v1.0	PP3. Training slides for organizations	PP3. Training slides for organizations
NTT_22-013_S4S+CYBER_PRE-v1.0	D2. Additional training material.	Video presenting the process models + a Brochure

Table 7 List of deliverables


NTT DATA
FUTURE
AT HEART